System Security

These topics describe the major security features of Prime Network and their configurable points:

- Communication Security, page 13-1
- Device Communication Security: SSH and SNMPv3, page 13-4
- Registry Security, page 13-6
- User Authentication and Authorization, page 13-6

Communication Security

Figure 13-1 illustrates the different forms of secure communication that are implemented between the Prime Network gateway server, units, clients, and database.
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.

If you upgrade your version of Prime Network, be sure to upgrade all components—gateway server, units, and clients—to avoid problems with connections.

For information on Prime Network Change and Configuration Management communication security, see Cisco Prime Network 3.8 Change and Configuration Management User Guide.

**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. The default encryption settings are as follows:

- Client-to-database connections are encrypted.
- Server-to-database connections are:
  - Encrypted if are using an embedded database. After installation, this can be changed by editing the registry.
  - Not encrypted for all other database installations, although you can change this (and choose an encryption type) at installation time.

The database schemas are described in the *Prime Network Database Schemas, page 10-1*. You can change database schema passwords using the procedure described in the *Changing Passwords: Prime Network Database Schemas, page 15-1*.

**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 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 Managing Configurations with Firewalls (Device Proxy), page 9-2.

Device Communication Security: 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. Protocols 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 13-1 summarizes the security methods that are supported by each protocol.

Table 13-1  Device Communication Security Features in SSHv1, SSHv2, and SNMPv3

<table>
<thead>
<tr>
<th>Protocol</th>
<th>Supported Security Feature for Device Communication</th>
</tr>
</thead>
<tbody>
<tr>
<td>SSHv1</td>
<td>Encryption ciphers: DES, 3DES, Blowfish</td>
</tr>
<tr>
<td>SSHv2</td>
<td>Client Authentication: password, public keys</td>
</tr>
<tr>
<td></td>
<td>Server Authentication Method: none, save-first-auth, preconfigured</td>
</tr>
<tr>
<td></td>
<td>Server Authentication Key: fingerprint or public key (not used if none is chosen for server authentication method)</td>
</tr>
<tr>
<td></td>
<td>Key exchange: DH-group1-sha1, DH-group1-exchange-sha1</td>
</tr>
<tr>
<td></td>
<td>MAC algorithm: SHA1, MD5, SHA1-96, MD5-96</td>
</tr>
<tr>
<td></td>
<td>Ciphers: 3DES, AES-128, AES-192, AES-256, Blowfish, Arcfour</td>
</tr>
<tr>
<td></td>
<td>Host Key Algorithm: DSA, RSA</td>
</tr>
<tr>
<td>SNMPv3</td>
<td>Authentication settings: NoAuthPriv (authentication without encryption), AuthPriv (authentication and encryption)</td>
</tr>
<tr>
<td></td>
<td>Ciphers: DES, AES128, AES192, AES256</td>
</tr>
<tr>
<td></td>
<td>Encryption algorithms: MD5, SHA</td>
</tr>
</tbody>
</table>

The settings in Table 13-1 can be controlled from Prime Network Administration, as described in VNE Telnet/SSH Settings, page 19-27. 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 13-1 are supported.
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.

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

### Step 1
Log into the gateway as `network-user` (where `network-user` is the operating system account for the Prime Network application, created when Prime Network is installed; for example, `network38`), 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"
```

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

```
# ./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.

User Authentication and Authorization

Note

These features are disabled if Prime Network is installed with Cisco Prime Central. If a user tries to log into Prime Network, they will be redirected to the suite login page. The only exception is the Prime Network emergency user, who will still be allowed to log into standalone Prime Network.

Prime Network uses a combination of methods to manage user authentication and authorization:

- **User authentication** can be managed locally by Prime Network or externally by an LDAP application. Either method can be used to validate user accounts and passwords, thus controlling who can log into Prime Network. If you use Prime Network, user information and passwords are stored in the Prime Network database. If you use an external LDAP application, passwords are stored on the external LDAP server. See Overview of User Authentication and Authorization, page 7-1.

- **User authorization** is managed through a combination of user access roles and scopes:
  - User access roles control the actions a user can perform in the Prime Network GUI clients. When a user’s account is created, the user is assigned an access role that determines the user’s default permissions. For more information, see Prime Network User Roles, page 7-2.
  - Scopes are groups of network elements that are created by administrators. Once a scope is created, you can assign it to users. A user’s default permissions determine the actions the user can perform on the network elements in the scope. These actions are referred to as the user’s security level on that scope. If desired, you can assign the user a more strict user access role for a scope. For more information, see Device Scopes, page 7-3.

When creating a user account, the password has to meet stringent rules. These rules can be set globally and are documented in Setting Global Password Rules, page 7-14. That topic also describes how administrators can specify how many login attempts are allowed, after which a user account is disabled. Administrators can also configure a period after which inactive accounts are disabled; see Automatically Disabling Accounts for Inactive Users, page 7-15.

Administrators can set up a daily message that is displayed when a user logs in. The message must be acknowledged to get to the login screen. For information, see Creating a GUI Client Banner Message, page 2-5.