Oracle® Corente Cloud Services Exchange

Administration Guide for Release 9.4.3

E76627-05
May 2017

Oracle Legal Notices

Table of Contents

Preface

The *Corente Services Administration Guide* provides details to help you administer and maintain your Corente Services network.

Related Documentation

The documentation for this product is available at:

http://www.oracle.com/technetwork/server-storage/corente/documentation/index.html

Feedback

Provide feedback about this documentation at:

http://www.oracle.com/goto/docfeedback

Conventions

Hyperlinks can be used to navigate through the guide or the procedures related to an overall activity, or to jump to a cross-referenced topic or Internet URL.

The following text conventions are used in this document:

Convention	Meaning
boldface	Boldface type indicates graphical user interface elements associated with an action, or terms defined in text or the glossary.
italic	Italic type indicates book titles, emphasis, or placeholder variables for which you supply particular values.
`monospace`	Monospace type indicates commands within a paragraph, URLs, code in examples, text that appears on the screen, or text that you enter.

Access to Oracle Support

Oracle customers that have purchased support have access to electronic support through My Oracle Support. For information, visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=info or visit http://www.oracle.com/pls/topic/lookup?ctx=acc&id=trs if you are hearing impaired.

Document Revision

Document generated on: 2017-05-01 (revision: 1222)

Chapter 1 Accessing Corente Cloud Services Exchange Components

Table of Contents

You use the following components to perform administrative tasks and monitor your Corente Services network:

App Net Manager

App Net Manager lets you manage and configure your Corente Services network. You can add and edit Gateway locations, define policies, control user access, set up third-party devices, and perform other tasks.

To access App Net Manager, do the following:

1. Go to: `https://www.corente.com/appnet`.
2. If prompted, open the Java Network Launch Protocol (`.jnlp`) file with the Java Web Start application.

   App Net Manager loads and then prompts you with the **Domain Authentication** window.
3. Specify the credentials and domain name with which you were provided.
4. Optionally select **Remember my User ID and Domain** and then select **Login**.

Gateway Viewer

Gateway Viewer lets you monitor network activity, diagnose and troubleshoot connectivity issues, and so on.

To access Gateway Viewer:

1. Go to: `http://`*`IP_Address`*.

   Where *`IP_Address`* is the LAN IP address of the Corente Services Gateway.

   Note

   To access Gateway Viewer from a different computer connected to your LAN, you must add the IP address of that computer to the default user group for the Location in App Net Manager. You must also ensure that no firewall policies block access to Gateway Viewer.
2. Log in with the following user name: `user`

For security purposes, this document does not provide any default user passwords. Contact Corente Cloud Services Exchange Support if you do not know the Gateway Viewer password.

1.1 Managing Credentials

Corente Cloud Services Exchange provides a set of default credentials for the Gateway Viewer. For App Net Manager, you specify root administrator credentials when your domain is created. You can then create other administrators in App Net Manager.

As a security best practice, you should change any default passwords immediately and configure password settings to suit your business requirements. You should also restrict access to administrative user credentials following the principle of least privilege.

To find out more about password settings and authentication in Corente Cloud Services Exchange, see the *Corente Services Security Guide*.

1.1.1 Changing Passwords

Complete the steps in this section to change passwords for Corente Cloud Services Exchange components.

1.1.1.1 Changing the App Net Manager Password

To change the password for a specific App Net Manager user, do the following:

1. Log in to App Net Manager as the user whose password you want to change.
2. Select **Login** and then select **Change Password**.
3. Enter the details for the new password and then select **OK**.

1.1.1.2 Changing the Gateway Viewer Password

To change the default user password for the Gateway Viewer, do the following:

1. Open the Gateway Viewer.
2. Select **Admin** and then select **Admin Login**.
3. Enter your administrator credentials.

   The Gateway Viewer administration pages display.
4. Select **Advanced** and then **Change Password**.

   The **Corente Services Gateway change password** page displays.
5. Enter and submit the new password.

1.1.2 Configuring Password Settings for Administrators

Complete the following steps to configure password settings, such as minimum password length, password expiration periods, and password reuse restrictions, for users with administrative privileges:

1. Open App Net Manager and log in as the root administrator.

2. Right-click the domain in the domain directory and then select **Preferences**.

   The **Preferences** dialog displays.

3. Select the **Password** tab.

4. Specify password settings as appropriate and then select **OK**.

The password settings apply to all users with administrator privileges. This includes App Net Manager users and the user for the Gateway Viewer.

1.2 Accessing App Net Manager or Gateway Viewer from Behind a Proxy Server

If your Corente Services Gateway is operating behind a proxy server, you must make sure that all Corente Services network users on your network change their web browser's settings to bypass the proxy server for local addresses and to specifically exclude the LAN IP address of the Corente Services Gateway.

This must be done for *every* computer that will have access to the Location gateway.

For example, if you are using Internet Explorer:

1. Go to the Tools menu and select Internet Options.

2. Select the Connections tab at the top of the window and click the LAN Settings button when it appears.

3. On this screen, make sure the *Use a proxy server* checkbox is checked. Fill in the IP Address and port fields for the proxy server and then make sure the *Bypass proxy server for local addresses* checkbox is checked.

4. Select the Advanced button in this Proxy Server section and add the LAN IP Address of your Location gateway to the Exceptions list.

5. Click OK on all screens to save these settings.

Important

To access App Net Manager, you must add `https://www.corente.com/appnet` to the proxy exceptions list in your web browser. You should not access App Net Manager through a proxy server.

Chapter 2 Setting Up Mobile Users

Table of Contents

You can add and configure mobile users in your Corente Services network.

2.1 Remote Access and Mobile Users

You provide remote and traveling users with Mobile User accounts in App Net Manager so that they can connect to Corente Services Gateways and access resources at your main office locations.

Mobile Users can remotely access a Corente Services network using:

- **Mobile Devices:** You configure secure mobile user access for iOS and Android devices in App Net Manager.
- **Oracle Corente Client:** Users with Microsoft Windows devices install a Corente Client that uses Internet Protocol Security (IPsec) for secure access.

2.2 Adding Mobile Users

You must add a Mobile User account for each user for whom you want to provide remote access to your Corente Services network. When you add Mobile User accounts, you organize them into Mobile User Groups so that you can associate groups of users with specific Locations.

To add Mobile Users to your Corente Services network, do the following:

1. Open App Net Manager.
2. Expand the **Global Intranet Settings** menu in the domain directory.
3. Expand **User Remote Access** and then expand **Mobile User Administration**.
4. Create a Mobile User Group, if necessary. You must create at least one Mobile User Group before you can add Mobile Users.
   a. Select **Mobile Users Groups** and then right-click and select **Add Mobile User Group**.

      The **Add Mobile User Group** dialog displays.

   b. Specify a name for the Mobile User Group and then select **OK**.
5. Select **Mobile Users** and then right-click and select **Add Mobile User**.

   The **Add Mobile User** dialog displays.

6. Specify the Mobile User details on the **Add Mobile User** dialog as appropriate. See the *App Net Manager Help* for detailed instructions.

   If Mobile Users use Microsoft Windows client devices, they must download and install the Corente Client. For these Mobile User accounts, you must:

   - Configure the **Windows Helper App Settings** section of the Mobile User Account and select **Use in conjunction with Windows Helper App**.
   - Specify passwords in the Mobile User accounts, even if you use an external authentication provider. Corente Clients use the passwords to authenticate with the Corente Services Control Point (SCP) to download and update their configurations.

7. Add the Mobile User to a Mobile User Group.

8. Select **OK** to close the **Add Mobile User** dialog and then save your changes.

After you create Mobile Users, Corente Cloud Services Exchange automatically sends notification emails to those users at the email addresses that you specify in the Mobile User accounts.

- If you configure settings in the **Windows Helper App Settings** section of the Mobile User account, the notification email instructs users to download and install the Corente Client.
- If you do not configure settings for the Corente Client, the notification email instructs users to configure VPN connections on their mobile devices.
- You cannot disable automatic notifications after you create Mobile Users. You also cannot change the text in the notification emails.
- You must provide Mobile Users with their passwords, if required. Passwords for Mobile Users are not specified in the notification emails.

2.3 Configuring Authentication for Mobile Users

Mobile Users authenticate to your Corente Services network using:

Password Authentication	Lets you define passwords in App Net Manager that Mobile Users must enter to connect to your Corente Services network. The Corente Services Control Point (SCP) stores the credentials and handles authentication when Mobile Users log in. You can use password authentication as an alternative to an external authentication provider for Mobile Users. However, you must always specify passwords for Mobile Users who run the Corente Client, even if you use an external authentication provider. Corente Clients use the passwords to authenticate with the Corente Services Control Point (SCP) to download and update their configurations.
External Authentication Provider	Uses an authentication provider on your LAN, such as a RADIUS server or Microsoft Active Directory server. Mobile Users must enter the credentials that you define in the authentication provider to connect to your Corente Services network.

To configure password authentication for Mobile Users, you specify the password in the Mobile User account. See Section 2.2, “Adding Mobile Users”.

To configure an external authentication provider, do the following:

1. Open App Net Manager.
2. Expand the **Locations** menu in the domain directory.
3. Expand the Location for which you want to configure an external authentication provider.
4. Expand **External Authentication** and then select either **LDAP Server** or **RADIUS Server**, as appropriate.
5. Right-click and select **Edit** to configure the external authentication provider.

   The **Edit * Server** dialog displays.
6. Configure the external authentication provider. See the *App Net Manager Help* for field descriptions and detailed instructions.
7. Select **OK** to close the **Edit * Server** dialog and then save your changes.

2.4 Adding Mobile Users as Location Partners

You must add each Mobile User Group as a partner of a Location. Adding Mobile Users as Location partners associates those users with specific Corente Services Gateways. Mobile Users can then connect over the Internet using secure tunnels to the Corente Services Gateways.

You configure the secure tunnels through which Mobile Users connect to Corente Services Gateways by adding one or more tubes. Tubes define firewall policies for connections between Mobile Users and Locations. Tubes also control access permissions between Mobile Users and computers, programs, and services on your LAN.

Note

- When Mobile Users connect to their host Locations, the Corente Services Gateways can enforce firewall policies on the local side of the connection only.
- You cannot configure Quality of Service (QoS) rules for Mobile Users.
- When you add a Mobile User Group as a partner of a Location, that Location becomes the host for those users. If the host Location has partnerships with other Locations in your Corente Services network, Mobile Users can also access those Locations only if you select the **Backhaul All Traffic** option when you add the Mobile Users.

To add Mobile User Groups as Location partners, do the following:

1. Open App Net Manager.
2. Expand the **Locations** menu in the domain directory.
3. Select the Location to which you want to partner Mobile Users.
4. Right-click the Location and then select **Edit**.

   The **Edit Location** window displays.
5. Enable the Location for Mobile User access and define an IPSec pre-shared key (PSK), if required.
   a. Select the **User Remote Access** tab on the **Edit Location** window.
   b. Select **Allow Mobile User Access to the Network** tab on the **User Remote Access** tab.

> **Note**
>
> You cannot partner Mobile Users to a Location if you do not select this option.

c. Specify the IPSec pre-shared key in the **Shared Secret** field.

   You should follow the PSK best practices to ensure network security. See the *Corente Services Security Guide*.

6. Select the **Partners** tab on the **Edit Location** window.
7. Select **Add** on the **Partners** tab.

   The **Add Partner** dialog displays.
8. Select **Mobile User Group** and then select the appropriate Mobile User Group from the drop-down menu item.
9. Select **Add** to add and configure a tube for the Mobile User Group.

   The **Add Tube** dialog displays.
10. Configure the tube with the appropriate settings. See the *App Net Manager Help* for field descriptions and detailed instructions.
11. Select **OK** to close the **Add Tube** dialog and then select **OK** to close the **Add Partner** dialog.
12. Select **OK** when you are finished making changes to the Location and then save your changes.

2.5 Setting Up Mobile User Devices

Mobile devices use native Layer 2 Tunneling Protocol (L2TP) to connect to Corente Services Gateways. You do not need to install separate software on mobile devices.

Mobile users with Microsoft Windows devices must install the Corente Client Software.

2.5.1 Ports for Mobile User Connections

Traffic between Mobile Users and Corente Services Gateways occurs on the following ports:

- UDP port 500
- UDP port 4500

2.5.2 Installing the Corente Client Software

Mobile Users with Microsoft Windows devices must install the Corente Client. The Corente Client is a lightweight agent that uses native IPSec functionality in the Windows operating system (OS) to securely connect to Corente Services Gateways.

> **Note**
>
> You must configure the **Windows Helper App Settings** section for Mobile User accounts in App Net Manager, otherwise those Mobile Users cannot use the Corente Client.

After you add Mobile Users, they receive notification emails to download the installation program for Corente Client from the following URL:

http://www.oracle.com/technetwork/server-storage/corente/downloads/index.html

The installation program for the Corente Client is `CorenteClient.exe`. A user with administrative privileges on either the local device or the domain must run the installation program. You should ensure that Microsoft Windows User Account Control (UAC) settings on the device do not prevent you from installing the Corente Client as an administrator.

2.5.3 Providing Mobile Users with Information

For Mobile Users to connect to your Corente Services network, you must provide them with the following information:

- Shared secret, or IPSec pre-shared key (PSK), for both mobile devices and the Corente Client.

  As a security best practice, you should not transmit the shared secret over the Internet. See the *Corente Services Security Guide* for more information.

- Password, if you do not use an external authentication provider. You must always define passwords for the Corente Client.

- Server address for Mobile Users to specify when they configure connection details in the the Corente Client.

Chapter 3 Monitoring Corente Services Gateways with SNMP

Table of Contents

Each Corente Services Gateway provides an SNMP interface that lets you poll the Location gateway and receive traps.

3.1 Configuring SNMP

You must configure SNMP for your Corente Services Gateway in App Net Manager. The following steps provide a high-level overview of how to configure SNMP:

1. Specify SNMP users and views in the **SNMP** folder under the **Global Intranet Settings** section of the domain directory.

2. For each Location in the domain for which you want to enable SNMP monitoring, navigate to the **SNMP** tab on the Location form and then:
   - Select **Enable SNMP at this Location**.
   - Select **Contact Information** and specify contact details as appropriate.
   - Add community polls as required.
   - Add community and user traps as required.

See the *App Net Manager Help* for complete details on configuring SNMP in App Net Manager.

3.2 Polling with the Corente MIB

The Corente MIB provides information specific to Corente Cloud Services Exchange.

3.2.1 Location Gateway Information

To view information about a specific Corente Services Gateway, you would poll *CORENTE-MIB::corente* and receive the following information about the Location gateway:

Table 3.1 Polling for Corente Services Gateway Information

Variable	Definition
gatewayDomain	The name of the domain in which the Location gateway exists.
gatewayName	The Gateway Name of the Corente Services Gateway.
gatewayConfig	The configuration type of the Corente Services Gateway or Corente Client (peer, inline, or client).
tunnelNumber	The number of tunnels that this Location gateway currently has.

Sample Poll Result:

```
enterprises.corente.gateway.gatewayDomain.0 = LargeCompany
enterprises.corente.gateway.gatewayName.0 = New_York
enterprises.corente.gateway.gatewayConfig.0 = inline
enterprises.corente.tunnels.tunnelNumber.0 = 2
```

3.2.2 Corente Tunnels

To view information about the tunnels of a Corente Services Gateway, you would poll *Corente-MIB::tunnelTable* and receive the following table with information about each tunnel that the Location gateway currently has to its partners:

Table 3.2 Polling for Information about a Corente Services Gateway's Tunnels

Variable	Definition
tunnelIndex	Reference number (row number) for the tunnel table.
tunnelPartnerName	The name of the partner.
tunnelPartnerConfig	The configuration type of the partner Location (peer, inline, native, or client).
tunnelStatus	The current status of the tunnel. • **TunnelUp:** The tunnel is UP.

Variable	Definition
	• **TunnelDown:** The tunnel is DOWN. • **TunnelPending:** The tunnel is attempting to be established. • **TunnelConfigAlert:** The tunnel has a configuration problem. • **TunnelConditional:** The tunnel is PARTIALLY UP but has experienced an IPSEC subnet failure. • **TunnelAlert:** The tunnel is DOWN and ALARMED due to LAN related problems. • **TunnelUnknown:** The tunnel state is presently UNKNOWN.
tunnelUptime	The amount of time (in seconds) since the tunnel last came up.
tunnelCumUptime	The cumulative length of time (in seconds) that this tunnel has been up since the Location gateway was last started.
tunnelNatEffect	The NAT settings currently active on the tunnel. The possible values in this field are defined as follows: • 0 – No NAT present • 1 – Auto Resolve enabled • 2 – Inbound NAT enabled • 4 – Outbound NAT enabled • 5 – Outbound NAT and Auto Resolve enabled • 6 – Outbound and Inbound NAT enabled
tunnelTransport	The transport protocol used to encapsulate packets (TCP, UDP, or native).
tunnelTransKB	The number of kilobytes transmitted by the Location gateway since the tunnel started.
tunnelTransPkts	The number of packets transmitted by the Location gateway since the tunnel started.
tunnelRecvKB	The number of kilobytes received by the Location gateway from its partner since the tunnel started.
tunnelRecvPkts	The number of packets received by the Location gateway from its partner since the tunnel started.
tunnelErrors	The number of packets that had errors since the tunnel started.
tunnelDropped	*Does not currently apply and is reserved for future use.*
tunnelQueued	The number of packets that have been queued (delayed transmission) since the tunnel started. The size of the tcptd packet queue at the moment when the poll is processing. The "high-water mark" for the number of packets that have been queued for transmission since the tunnel started.

Sample Poll Result:

```
SNMP table: enterprises.corente.tunnels.tunnelTable
    tunnelIndex        tunnelPartnerName     tunnelPartnerConfig     tunnelStatus
              1          LA.LargeCompany                    peer         tunnelUp
              2     Chicago.OtherCompany                  inline       tunnelDown

    tunnelUptime     tunnelCumUptime     tunnelNatEffect     tunnelTransport     tunnelTransKB
   10429 seconds       10429 seconds                   4                 UDP     244 kilobytes
       0 seconds           0 seconds                   0                 UDP       0 kilobytes

    tunnelTransPkts     tunnelRecvKB     tunnelRecvPkts     tunnelErrors     tunnelDropped
       2359 packets    241 kilobytes       2353 packets        0 packets         0 packets
          0 packets      0 kilobytes          0 packets        0 packets         0 packets

  tunnelQueued
     0 packets
     0 packets
```

3.2.3 Monitored Applications

To view information about applicatons being monitored by a Corente Services Gateway, you would poll *Corente-MIB::applications* or *Corente-MIB::applications.applicationTable* and receive the following table with information about each application that the Location gateway is currently monitoring:

Table 3.3 Polling for Information about Applications Monitored by a Corente Services Gateway

Variable	Definition
appIndex	Reference number (row number) for the application table.
appDisplayName	The name of the monitored application.
appStatus	The current status of the monitored application.
appComment	The comment that is currently enabled for the monitored application.
appVpnShare	Whether or not the application is shared over the secure network.

3.2.4 Monitored Services

To view further information about an application or service that is monitored by a Corente Services Gateway, you would poll *Corente-MIB::applications* or *Corente-MIB::applications.serviceDetailTable* and receive the following table with information about each service:

Table 3.4 Polling for Information about Services Monitored by a Corente Services Gateway

Variable	Definition
svcIndex	Reference number (row number) for the service table.
svcAppName	The name of the monitored application service.
svcPortNumber	The service port.
svcDisplayName	The service name.
svcProtocol	The service protocol (TCP or UDP).
svcHostName	The name of the machine that hosts the service.
svcIpAddr	The IP address of the machine that hosts the service.
svcStatus	The current status of the service.
svcLatencyMilliSec	The latency of the service (in milliseconds).
svcLastVerifyTime	The time that the current status of the service was last verified. The format is `yyyy/mm/dd HH:MM:SS`.

3.2.5 NATS

To get inbound and outbound addressing for the Corente Services Gateway, poll *Corente-MIB::nats*. This object returns the following:

Table 3.5 Polling for NAT Information for a Corente Services Gateway

Variable	Definition
natIndex	Reference number, or row number, for the NAT table
natDirection	Either Outbound (1) or Inbound (2)
natAcl	Access control list
natNatAcl	NAT access control list
natPartner	Name of the partner
natPartnerVip	Virtual IP (VIP) of the partner

3.3 Polling with Other MIBs

The following polls from MIBs other than the Corente MIB will also provide information about the Corente Services Gateway. In general, for definitions of variables in other MIBs, see the MIB or RFC associated with that MIB.

3.3.1 System Information

To find out the general system information about the Corente Services Gateway, you can poll *mib-2.system*.

Sample Result:

```
system.sysDescr.0 = Linux New_York 2.4.20-13.8or13 #1 Mon Dec 8 13:09:37 EDT 2003 i686
system.sysObjectID.0 = OID: enterprises.8072.3.2.10
system.sysUpTime.0 = Timeticks: (111287) 0:18:32.87
system.sysContact.0 = Sally Thompson|sthompson@largecompany.com|555-555-5555
system.sysName.0 = New_York
system.sysLocation.0 = 123 Main Street|New York City|NY|12345|US
```

The Unix `top` utility also provides good indicators to the utilization of the processors, processes, memory, and swap spaces. The top five lines of Linux `top` utility are covered by SNMP polls.

- **Uptime:** The first line displays the time the system has been up and the three load averages for the system. They are the average number of process ready to run during the last 1, 5, and 15 minutes since the system has been up.
- **Processes:** The second line displays the total number of processes running at the time of the last update.
- **CPU states:** The third line displays the percentage of the CPU time in user mode, system mode, niced tasks, and idle.
- **Mem:** The fourth displays statistics on memory usage.
- **Swap:** The fifth line displays swap space.

A sample `top` screen is shown below.

```
2:26pm up 2 days, 4:09, 3 users, load average: 0.93, 0.82, 0.65
128 processes: 126 sleeping, 2 running, 0 zombie, 0 stopped
CPU states: 50.1% user, 29.4% system, 0.0% nice, 20.3% idle
Mem: 255684K av, 82224K used, 173460K free, 0K shrd, 3776K buff
```

```
Swap: 40120K av, 19536K used, 20584K free 21712K cached

PID     USER   PRI NI   SIZE   RSS   SHARE   STAT   %CPU   %MEM   TIME   COMMAND
28868   root   18   0   37448   36M    148      R   79.0   14.6  20:58   dummy
28888   root   11   0    1032  1032    732      R    0.3    0.4   0:00   top
    6   root    9   0       0     0      0     SW    0.1    0.0   0:08   kscand
    1   root    8   0     116    52     40      S    0.0    0.0   0:04   init
    2   root    9   0       0     0      0     SW    0.0    0.0   0:00   keventd
    3   root    9   0       0     0      0     SW    0.0    0.0   0:00   kapmd
    4   root   19  19       0     0      0    SWN    0.0    0.0   0:00   ksoftirqd_CPU0
    5   root    9   0       0     0      0     SW    0.0    0.0   0:00   kswapd
    7   root    9   0       0     0      0     SW    0.0    0.0   0:00   bdflush
    8   root    9   0       0     0      0     SW    0.0    0.0   0:00   kupdated
   99   root    9   0       0     0      0     SW    0.0    0.0   0:00   kjournald
  100   root    9   0       0     0      0     SW    0.0    0.0   0:03   kjournald
  208   root    9   0     216   156    112      S    0.0    0.0   0:03   syslogd
  212   root    9   0     188   116    116      S    0.0    0.0   0:00   klogd
  221   rpc     9   0      88     0      0     SW    0.0    0.0   0:00   portmap
  467   root    9   0     232     0      0     SW    0.0    0.0   0:04   sshd
  483   root    9   0    1320    64     48      S    0.0    0.0   0:01   httpd
```

3.3.2 System Uptime

To poll for information that is on the first line of the `top` display, you can poll the MIBs: *HOST-RESOURCES-MIB* and *UCB-SNMP-MIB*.

General information about the host is available in the *host.hrSystem* subtree.

Poll: HOST-RESOURCES-MIB::host.hrSystem (.1.3.6.1.2.1.25.1)

Sample Poll Result:

```
host.hrSystem.hrSystemUptime.0 = Timeticks: (19133140) 2 days, 5:08:51.40
host.hrSystem.hrSystemDate.0 = 2003-6-5,15:25:42.0,+0:0
host.hrSystem.hrSystemInitialLoadDevice.0 = 1536
host.hrSystem.hrSystemInitialLoadParameters.0 = "auto BOOT_IMAGE=linux-clone \
ro root=301 BOOT_FILE=/clone/boot/vmlinuz."
host.hrSystem.hrSystemNumUsers.0 = Gauge32: 3
host.hrSystem.hrSystemProcesses.0 = Gauge32: 128
host.hrSystem.hrSystemMaxProcesses.0 = 0
```

Load average information is available in the table *ucdavis.laTable*.

Poll: UCB-SNMP-MIB::ucdavis.laTable (.1.3.6.1.4.1.2021.10)

Sample Poll Result:

```
SNMP table: enterprises.ucdavis.laTable
 laIndex laNames laLoad laConfig laLoadInt laLoadFloat laErrorFlag laErrMessage
 1 Load-1 0.69 12.00 68 0.690000 0 0
 2 Load-5 0.78 12.00 78 0.780000 0 0
 3 Load-15 0.74 12.00 73 0.740000 0 0
```

3.3.3 CPU States

To poll for the information on the third line of the `top` display, you can poll *UCBSNMP-MIB.ucdavis.systemStats* twice. Do not poll *ssCpuUser*, *ssCpuSystem*, *ssCpuIdle* because they are deprecated and replaced by *ssCpuRawUser*, *ssCpuRawSystem*, *ssCpuRawIdle*, and *ssCpuRawNice*.

Poll: UCB-SNMP-MIB.ucdavis.systemStats (.1.3.6.1.4.1.2012.11)

Sample First Poll Result at time t0:

```
enterprises.ucdavis.systemStats.ssIndex.0 = 1
enterprises.ucdavis.systemStats.ssErrorName.0 = systemStats
```

```
enterprises.ucdavis.systemStats.ssSwapIn.0 = 0
enterprises.ucdavis.systemStats.ssSwapOut.0 = 1
enterprises.ucdavis.systemStats.ssIOSent.0 = 0
enterprises.ucdavis.systemStats.ssIOReceive.0 = 1
enterprises.ucdavis.systemStats.ssSysInterrupts.0 = 114
enterprises.ucdavis.systemStats.ssSysContext.0 = 38
enterprises.ucdavis.systemStats.ssCpuUser.0 = 0
enterprises.ucdavis.systemStats.ssCpuSystem.0 = 0
enterprises.ucdavis.systemStats.ssCpuIdle.0 = 99
enterprises.ucdavis.systemStats.ssCpuRawUser.0 = Counter32: 29954
enterprises.ucdavis.systemStats.ssCpuRawNice.0 = Counter32: 0
enterprises.ucdavis.systemStats.ssCpuRawSystem.0 = Counter32: 25187
enterprises.ucdavis.systemStats.ssCpuRawIdle.0 = Counter32: 18585381
```

Sample Second Poll Result at time t1 where t1>t0:

```
enterprises.ucdavis.systemStats.ssIndex.0 = 1
enterprises.ucdavis.systemStats.ssErrorName.0 = systemStats
enterprises.ucdavis.systemStats.ssSwapIn.0 = 0
enterprises.ucdavis.systemStats.ssSwapOut.0 = 1
enterprises.ucdavis.systemStats.ssIOSent.0 = 0
enterprises.ucdavis.systemStats.ssIOReceive.0 = 1
enterprises.ucdavis.systemStats.ssSysInterrupts.0 = 114
enterprises.ucdavis.systemStats.ssSysContext.0 = 38
enterprises.ucdavis.systemStats.ssCpuUser.0 = 0
enterprises.ucdavis.systemStats.ssCpuSystem.0 = 0
enterprises.ucdavis.systemStats.ssCpuIdle.0 = 99
enterprises.ucdavis.systemStats.ssCpuRawUser.0 = Counter32: 32787
enterprises.ucdavis.systemStats.ssCpuRawNice.0 = Counter32: 0
enterprises.ucdavis.systemStats.ssCpuRawSystem.0 = Counter32: 26681
enterprises.ucdavis.systemStats.ssCpuRawIdle.0 = Counter32: 18586494
```

The raw numbers represent the actual CPU ticks between the two polls. You can use these numbers to compute the best statistics on average CPU utilization over a period of time. Below is an example on how to compute the average CPU utilization:

To compute average CPU utilization over a period of t1 – t0:

```
Total CPU ticks for users = ssCpuRawUser at t1 – ssCpuRawUser at t0 = 2833
Total CPU ticks for niced tasks = ssCpuRawNice at t1 – ssCpuRawNice at t0 = 0
Total CPU ticks for system = ssCpuRawSystem at t1 – ssCpuRawSystem at t0 = 1494
Total CPU ticks for idle = ssCpuRawIdle at t1 – ssCpuRawIdle at t0 = 1113
Total CPU ticks between t0 and t1 = 2833 + 0 + 1494 + 1113 = 5440
CPU user% = 2833/5440 x 100 = 52.08%
CPU system% = 1494/5440 x 100 = 27.46%
CPU nice% = 0/5440 x 100 = 0%
CPU idle% = 1113/5440 x 100 = 20.46%
Average CPU utilization over a period of t1 – t0 = 52.08 + 27.46 + 0% = 79.54%
```

3.3.4 Memory and Swap Space

To poll for the information on the fourth and fifth lines of the `top` display, you can poll *UCB-SNMP-MIB.ucdavis.memory*.

Poll: UCD-SNMP-MIB::ucdavis.memory

Sample Poll Result:

```
enterprises.ucdavis.memory.memIndex.0 = 0
enterprises.ucdavis.memory.memErrorName.0 = swap
enterprises.ucdavis.memory.memTotalSwap.0 = 40120
enterprises.ucdavis.memory.memAvailSwap.0 = 25316
enterprises.ucdavis.memory.memTotalReal.0 = 255684
enterprises.ucdavis.memory.memAvailReal.0 = 5004
enterprises.ucdavis.memory.memTotalFree.0 = 30288
```

```
enterprises.ucdavis.memory.memMinimumSwap.0 = 16000
enterprises.ucdavis.memory.memShared.0 = 0
enterprises.ucdavis.memory.memBuffer.0 = 7512
enterprises.ucdavis.memory.memCached.0 = 26976
enterprises.ucdavis.memory.memSwapError.0 = 0
enterprises.ucdavis.memory.memSwapErrorMsg.0 =
```

The poll results translate as follows to the variables in the Linux `top` command:

```
Memory available = memTotalReal = 255684 Kb
Memory used = memTotalReal – memAvailReal = 255684 – 5004 = 250680 Kb
Memery free = memAvailReal = 5005 Kb
Memory shared = memShared = 0
Memory buffer = memBuffer = 7512 Kb

Swap available = memTotalSwap = 40120 Kb
Swap used = memTotalSwap – memAvailSwap = 14804 Kb
Swap free = memAvailSwap = 25316 Kb
Swap cached = memCached = 26976 Kb

Mem: 255684K av, 82224K used, 173460K free, 0K shrd, 3776K buff
Swap: 40120K av, 19536K used, 20584K free, 21712K cached
```

3.3.5 Processes

To view the processes that are currently running on a Corente Services Gateway, you would poll *HOST-RESOURCES-MIB::host.hrSWRun.hrSWRunTable*.

The *hrSWRunTable* contains an entry for each distinct piece of software that is running or loaded into physical or virtual memory of the Location gateway in preparation for running. This includes the Location gateway's operating system, device drivers, and applications.

Sample Poll Result:

```
SNMP table: host.hrSWRun.hrSWRunTable

hrSWRunIndex  hrSWRunName  hrSWRunID  hrSWRunPath  hrSWRunParameters  hrSWRunType  hrSWRunStatus

1             "init"       .ccitt.ze  "init [3]"   ""                 application  runnable
2             "keventd"    .ccitt.ze  "keventd"    ""                 application  runnable
:
:
208           "syslogd"    .ccitt.ze  "syslogd"    "-m 0"             application  runnable
15186         "or-restart" .ccitt.ze  "/usr/lo.."  "-d 30 -r /etc.."  application  runnable
15188         "tcptd"      .ccitt.ze  "/usr/lo.."  "--udp --port .."  application  runnable
15296         "pluto"      .ccitt.ze  "/usr/lo.."  "--nofork --de.."  application  runnable
15357         "sessmgr"    .ccitt.ze  "/usr/lo.."  "--local --tim.."  application  runnable
15365         "redird"     .ccitt.ze  "/usr/lo.."  "-f /usr/local.."  application  runnable
15403         "org"        .ccitt.ze  "/usr/lo.."  "-f /usr/local.."  application  runnable
15404         "localdb"    .ccitt.ze  "/usr/lo.."  ""                 application  runnable
28729         "snmpd"      .ccitt.ze  "/usr/sb.."  "-s -f -P /var.."  application  running
28868         "dummy"      .ccitt.ze  "./dummy"    "32 200"           application  running

Number of processes = number of hrSWRunTable entries
Number of sleeping processes = number of hrSWRuntable entries that have hrSWRunStatus=runnable
Number of running processes = number of hrSWRuntable entries that have hrSWRunStatus=running
Number of zombie processes = number of hrSWRuntable entries that have hrSWRunStatus=invalid
Number of stopped processes = number of hrSWRuntable entries that have hrSWRunStatus=notRunnable
```

3.3.6 Network Interfaces

By polling for interface information with MIB-II (*mib-2.interfaces.ifTable*), you can view information about each network interface on a Corente Services Gateway. Interfaces commonly revealed are `eth0`, `eth1`, `tcpt0`, `ipsec0`, and `ipsec1`.

- `eth0` and `eth1`: The physical interfaces for either the LAN or the WAN.
- `tcpt0`: The virtual network interface used for all tunnel traffic.
- `ipsec0` and `ipsec1`: The virtual network interfaces for all IPSec traffic.

The interface `tcpt0`, `ipsec0` and `ipsec1` are not physical; they are virtual network interfaces. All Corente Services network tunnel traffic goes through the `tcpt0` interface. The statistical information of `tcpt0` is the aggregate of all Corente Services network tunnels. For example, the sum of all *corente.tunnelRecvKb* should be approximately equal to the *ifInOctects* value of the `tcpt0` entry. Similarly, if the *ifInErrors* or *ifOurErrors* value of `tcpt0` is greater than zero, we know that at least one of the Corente Services network tunnels has problems.

To monitor data for Corente Services network tunnels, monitor `tcpt0`. In the Corente MIB, *corente.tunnelTable* is a refinement of this `tcpt0` entry.

Sample Poll Result:

```
SNMP table: interfaces.ifTable

ifIndex ifDescr ifType ifMtu ifSpeed ifPhysAddress
1 lo softwareLoopback 16436 10000000 10000000
2 eth0 ethernetCsmacd 1500 10000000 0:1:3:1c:97:c9
3 tcpt0 ethernetCsmacd 1400 10000000 0:54:43:50:54:30
4 ipsec0 ethernetCsmacd 16260 10000000 0:54:43:50:54:30
5 ipsec1 ethernetCsmacd 16260 10000000 0:1:3:1c:97:c9
6 ipsec2 tunnel 0 0 0
7 ipsec3 tunnel 0 0 0

ifAdminStatus  ifOperStatus  ifLastChange  ifInOctets  ifInUcastPkts  ifInNUcastPkts
           up            up             ?      197681           2062               ?
           up            up             ?   966949898        2603112               ?
           up            up             ?     4251992          40785               ?
           up            up             ?     1969784          40714               ?
           up            up             ?           0              0               ?
         down          down             ?           0              0               ?
         down          down             ?           0              0               ?

ifInDiscards  ifInErrors  ifInUnknownProtos  ifOutOctets  ifOutUcastPkts
           0           0                  ?       197681            2062
           0           0                  ?     13425106          110277
           0           0                  ?      4689744           41135
           0           0                  ?      5255638           40841
           0           0                  ?            0               0
           0           0                  ?            0               0
           0           0                  ?            0               0

ifOutNUcastPkts  ifOutDiscards  ifOutErrors  ifOutQLen          ifSpecific
              ?              0            0          0  .ccitt.zeroDotZero
              ?              0            0          0  .ccitt.zeroDotZero
              ?              0            0          0  .ccitt.zeroDotZero
              ?            293            0          0  .ccitt.zeroDotZero
              ?              0            0          0  .ccitt.zeroDotZero
              ?              0            0          0  .ccitt.zeroDotZero
              ?              0            0          0  .ccitt.zeroDotZero
```

3.3.7 IP Addresses

To view the IP addresses assigned to a Corente Services Gateway, you would poll *mib-2.ip.ipAddrTable*. The IP address table is displayed, which contains this Location gateway's IP addressing information.

Sample Poll Result:

```
SNMP table: ip.ipAddrTable
```

```
    ipAdEntAddr  ipAdEntIfIndex  ipAdEntNetMask  ipAdEntBcastAddr  ipAdEntReasmMaxSize
        0.0.0.0               6         0.0.0.0                 0                    ?
    10.0.24.167               3       255.0.0.0                 1                    ?
      127.0.0.1               1       255.0.0.0                 0                    ?
192.168.164.223               2   255.255.192.0                 1                    ?
```

3.3.8 Routes

To view the routes that are configured for the Location gateway to get to its various LAN subnets, you would poll *mib-2.ip.ipRouteTable*. The IP routing table is displayed, which contains an entry for each route presently known to this Corente Services Gateway.

Sample Poll Result:

```
SNMP table: ip.ipRouteTable

  ipRouteDest  ipRouteIfIndex  ipRouteMetric1  ipRouteMetric2  ipRouteMetric3  ipRouteMetric4
      0.0.0.0               2               1               ?               ?               ?
     10.0.0.0               4               0               ?               ?               ?
 172.16.246.0               2               1               ?               ?               ?
 172.16.250.0               4               0               ?               ?               ?
192.168.128.0               2               0               ?               ?               ?

 ipRouteNextHop ipRouteType ipRouteProto ipRouteAge   ipRouteMask ipRouteMetric5        ipRouteInfo
  192.168.165.1    indirect        local       ?          0.0.0.0           ?    .ccitt.zeroDotZero
        0.0.0.0      direct        local       ?        255.0.0.0           ?    .ccitt.zeroDotZero
192.168.164.136    indirect        local       ?    255.255.255.0           ?    .ccitt.zeroDotZero
        0.0.0.0      direct        local       ?    255.255.255.0           ?    .ccitt.zeroDotZero
        0.0.0.0      direct        local       ?    255.255.192.0           ?    .ccitt.zeroDotZero
```

3.3.9 IP Information

To view IP information about the Location gateway, you would poll *mib-2.ip*.

Sample Poll Result:

```
ip.ipForwarding.0 = forwarding(1)
ip.ipDefaultTTL.0 = 64
ip.ipInReceives.0 = Counter32: 15603
ip.ipInHdrErrors.0 = Counter32: 0
ip.ipInAddrErrors.0 = Counter32: 0
ip.ipForwDatagrams.0 = Counter32: 0
ip.ipInUnknownProtos.0 = Counter32: 0
ip.ipInDiscards.0 = Counter32: 0
ip.ipInDelivers.0 = Counter32: 10827
ip.ipOutRequests.0 = Counter32: 8105
ip.ipOutDiscards.0 = Counter32: 0
ip.ipOutNoRoutes.0 = Counter32: 0
ip.ipReasmTimeout.0 = 0
ip.ipReasmReqds.0 = Counter32: 47
ip.ipReasmOKs.0 = Counter32: 23
ip.ipReasmFails.0 = Counter32: 0
ip.ipFragOKs.0 = Counter32: 46
ip.ipFragFails.0 = Counter32: 0
ip.ipFragCreates.0 = Counter32: 94
```

3.3.10 TCP Connections

To view the TCP connections of the Location gateway, you would poll *mib-2.tcp.tcpConnTable*.

The TCP connection table is displayed, which contains information about this Location gateway's existing TCP connections.

Sample Poll Result:

```
SNMP table: tcp.tcpConnTable

tcpConnState  tcpConnLocalAddress  tcpConnLocalPort  tcpConnRemAddress  tcpConnRemPort
      listen              0.0.0.0                22            0.0.0.0               0
      listen              0.0.0.0                80            0.0.0.0               0
      listen              0.0.0.0               111            0.0.0.0               0
      listen              0.0.0.0               199            0.0.0.0               0
      listen              0.0.0.0               443            0.0.0.0               0
      listen              0.0.0.0               551            0.0.0.0               0
      listen              0.0.0.0               900            0.0.0.0               0
      listen              0.0.0.0              8000            0.0.0.0               0
 established          10.0.24.167               900         10.0.22.40            1137
 established          10.0.24.167             32866     208.185.38.242            3000
 established      192.168.164.223                22     192.168.165.96           32956
 established      192.168.164.223                22     192.168.165.96           32959
 established      192.168.164.223               551       172.16.250.4            1136
 established      192.168.164.223             32865     172.16.254.158             551
```

3.3.11 TCP Information

To view the TCP information of the Location gateway, you would poll *mib-2.tcp*. The TCP group is displayed. Note that instances of object types that represent information about a particular TCP connection are transient; they persist only as long as the connection in question.

Sample Poll Result:

```
tcp.tcpRtoAlgorithm.0 = other(1)
tcp.tcpRtoMin.0 = 200
tcp.tcpRtoMax.0 = 120000
tcp.tcpMaxConn.0 = -1
tcp.tcpActiveOpens.0 = Counter32: 6
tcp.tcpPassiveOpens.0 = Counter32: 6
tcp.tcpAttemptFails.0 = Counter32: 0
tcp.tcpEstabResets.0 = Counter32: 1
tcp.tcpCurrEstab.0 = Gauge32: 4
tcp.tcpInSegs.0 = Counter32: 682
tcp.tcpOutSegs.0 = Counter32: 745
tcp.tcpRetransSegs.0 = Counter32: 4
```

3.3.12 UDP Listening Ports

To view the UDP listening ports of the Location gateway, you would poll *mib-2.udp.udpTable*.

The UDP listener table is displayed, which contains information about this Location gateway's UDP end-points which are currently accepting datagrams.

Sample Poll Result:

```
SNMP table: udp.udpTable

 udpLocalAddress  udpLocalPort
         0.0.0.0            68
         0.0.0.0           111
         0.0.0.0           161
         0.0.0.0           551
         0.0.0.0           900
         0.0.0.0           902
         0.0.0.0           907
         0.0.0.0           908
         0.0.0.0           912
         0.0.0.0          1010
```

```
         0.0.0.0         32791
         0.0.0.0         32795
         0.0.0.0         32796
         0.0.0.0         32797
     10.0.24.167           500
       127.0.0.1           901
       127.0.0.1           920
 192.168.164.223           137
 192.168.164.223           500
```

3.3.13 UDP Information

To view the UDP information of the Location gateway, you would poll *mib-2.udp*.

Sample Poll Result:

```
udp.udpInDatagrams.0 = Counter32: 6757
udp.udpNoPorts.0 = Counter32: 106
udp.udpInErrors.0 = Counter32: 0
udp.udpOutDatagrams.0 = Counter32: 6371
```

3.3.14 ICMP Information

To view the ICMP information of the Location gateway, you would poll *mib-2.icmp*.

Sample Poll Result:

```
icmp.icmpInMsgs.0 = Counter32: 2445
icmp.icmpInErrors.0 = Counter32: 0
icmp.icmpInDestUnreachs.0 = Counter32: 111
icmp.icmpInTimeExcds.0 = Counter32: 0
icmp.icmpInParmProbs.0 = Counter32: 0
icmp.icmpInSrcQuenchs.0 = Counter32: 0
icmp.icmpInRedirects.0 = Counter32: 0
icmp.icmpInEchos.0 = Counter32: 1287
icmp.icmpInEchoReps.0 = Counter32: 1047
icmp.icmpInTimestamps.0 = Counter32: 0
icmp.icmpInTimestampReps.0 = Counter32: 0
icmp.icmpInAddrMasks.0 = Counter32: 0
icmp.icmpInAddrMaskReps.0 = Counter32: 0
icmp.icmpOutMsgs.0 = Counter32: 1423
icmp.icmpOutErrors.0 = Counter32: 0
icmp.icmpOutDestUnreachs.0 = Counter32: 136
icmp.icmpOutTimeExcds.0 = Counter32: 0
icmp.icmpOutParmProbs.0 = Counter32: 0
icmp.icmpOutSrcQuenchs.0 = Counter32: 0
icmp.icmpOutRedirects.0 = Counter32: 0
icmp.icmpOutEchos.0 = Counter32: 0
icmp.icmpOutEchoReps.0 = Counter32: 1287
icmp.icmpOutTimestamps.0 = Counter32: 0
icmp.icmpOutTimestampReps.0 = Counter32: 0
icmp.icmpOutAddrMasks.0 = Counter32: 0
icmp.icmpOutAddrMaskReps.0 = Counter 32: 0
```

3.4 Traps

Each Corente Services Gateway can be configured to send SNMP traps when certain alarms or events occur on the Location gateway or on any of its tunnels. On the Alerts tab of the Location form for each Location gateway, you can select the trap categories you want to receive and the ones to filter. You can also filter traps via your trap listener application. Each trap is assigned a level of severity.

3.4.1 Alarm Traps

When a problem occurs that affects service, an alarm trap will be generated. There are three levels of alarm traps:

- **Critical:** The Location gateway is unable to start.
- **Major:** The Location gateway can start, but is prevented from functioning correctly.
- **Minor:** Nothing prevents the Location gateway from starting up or functioning.

Receivers of the alarm traps should assume that there are problems with the Location gateway services and should keep themselves in an alert state until the traps are cleared. A Corente Services Gateway will notify of cleared alarms by sending out traps designated as *clear*. Each trap category has its alarms and clears.

Traps are not fully reliable because they are delivered using UDP packages. Network outages or the unavailability of listeners or agents could affect the trap delivery. The Corente Services Gateway will do its best by resending alarms at 15-minute intervals if they have not been cleared. It is the receiver's responsibility to determine with polling the status of long-term, un-cleared major or critical alarms. Some major or critical alarm traps have associated poll objects that can determine if they are cleared. Some traps do not have associated poll objects because the condition may be so serious that the Location gateway SNMP agent (or even the Corente Services Gateway itself) is down and not answering polls.

When a listener receives a clear trap and finds no raised alarms, it should ignore the trap.

3.4.2 Event Traps

In addition to the alarm traps, there will be two additional levels that deal with events. When something has happened that requires attention but has no impact to the Location gateway services, event traps are generated.

- **Clear:** An alarm trap has cleared.
- **Info:** An event has occurred that is not an alarm or a clear.

Unlike alarms, events need no clears. Receivers should take advisory actions when event traps are received.

Event traps are sent once when the event has happened. No further attempt is taken on the Corente Services Gateway or the receivers to make sure that the delivery of an event is successful.

3.4.3 Traps to Expect

The traps to expect when Corente Services networks are functioning normally are as follows:

There are two event traps that signal the birth and death of the Corente Services Gateway SNMP agent. The trap *coldStart* indicates the start of the agent and the trap *nsNotifyShutdown* indicates the termination of the agent. All alarm traps that are associated with the Location gateway are cleared when the listeners receives either of these traps.

- **On Shutdown:** When a Location gateway starts a normal shutdown, the first trap that is generated is the *shutdownStartTrap* trap. After this trap, a series of predictable traps will follow, such as the *partnerDownTrap* trap for each tunnel of this Location gateway that is brought down due to the Location gateway shutting down. A listener can choose to ignore these upcoming traps until *nsNotifyShutdowTrap* is received.
- **On Startup:** When a Location gateway is booted, the first trap received will be the *coldStart* trap. Then, the Location gateway tries to establish Corente Services network tunnels to its partners. It

indicates to listeners the operational status of the tunnels by sending either the *partnerUpTrap* trap or *partnerDownTrap* trap.

3.4.4 Important Traps to Monitor

The most important traps to look for will be *partnerUpTrap* and *partnerDownTrap*, which will alert you if connections between locations have been interrupted.

3.5 Trap Severity Details

The following tables list the traps that you may receive, their severity level, and how you will be notified that they have cleared (by traps that you may receive and by polls that you can make to the associated Location gateways).

3.5.1 Configuration Traps

Table 3.6 Guide to Configuration Traps

Trap OID and Definition	Severity	(When Cleared) Traps Received	(When Cleared) Polling Information
configChangeTrap Corente Services Gateway configuration has been changed.	info	N/A	N/A
configOpen551Trap Neither side permits an inbound connection.	major	configTunClearTrap	TunnelTable entry, status is tunnelUp
configSubnetCnfTrap Corente Services Gateway's partner has reported a Corente Services network subnet failure.	major	configTunClearTrap	TunnelTable entry, status is tunnelUp
configNatPolicyTrap The NAT policy between this Corente Services Gateway and its partner is in conflict. For example, one side has a NAT policy of 'prohibited' and the other side has a 'specified' inbound or outbound NAT policy.	major	configTunClearTrap	TunnelTable entry, status is tunnelUp
configNoInbSpaceTrap Inbound NAT policy is specified for the partner tunnel, but no available inbound space has been found to satisfy the request.	major	configTunClearTrap	TunnelTable entry, status is tunnelUp
configNoMagSpaceTrap Auto Resolve is required for the declared range, but there is insufficient space in	major	configTunClearTrap	TunnelTable entry, status is tunnelUp

Trap OID and Definition	Severity	(When Cleared) Traps Received	(When Cleared) Polling Information
the Auto Resolve pools to satisfy the request.			
configNatPrhbtTrap Auto Resolve policy is disabled, so the declared range will not be NAT-ed to a non-conflicting address.	major	configTunClearTrap	TunnelTable entry, status is tunnelUp
configAddrCnfTrap Auto Resolve policy is disabled, and the declared range conflicts with or overlaps an address range already in use from the third Corente Services Gateway.	major	configTunClearTrap	TunnelTable entry, status is tunnelUp
configAddrNestedTrap Auto Resolve policy is disabled, and the declared range nests inside an address range already in use from the third Corente Services Gateway.	major	configTunClearTrap	TunnelTable entry, status is tunnelUp
configAddrCmmtdTrap The declared range is in conflict with an already committed inbound address range.	major	configTunClearTrap	TunnelTable entry, status is tunnelUp
configInbAddrCnfTrap The declared inbound NAT address conflicts with the Corente Services Gateway's local User Group definition.	major	configTunClearTrap	TunnelTable entry, status is tunnelUp
configDhcpFailTrap Client could not acquire an IP address from the Corente Services Gateway via DHCP.	major	configClearTrap	N/A
configRasCnfTrap Partner does not accept RAS connections.	major	configClearTrap	N/A
configLclAddrCnfTrap Local address ranges conflict with one another, due to their NAT policies.	major	configClearTrap	N/A
configTubeFailTrap Unknown User Group.	major	configTunClearTrap	TunnelTable entry, status is tunnelUp
configNoNatExtLinkTrap NAT is not permitted on external links.	major	configTunClearTrap	TunnelTable entry, status is tunnelUp

Trap OID and Definition	Severity	(When Cleared) Traps Received	(When Cleared) Polling Information
configTunClearTrap This trap clears the tunnel configuration alarm trap identified by the partnerFullname.	clear	N/A	N/A
configClearTrap This trap clears all Location gateway configuration alarm traps.	clear	N/A	N/A
configIpsecDevTrap IPsec device is misconfigured.	major	configTunClearTrap	TunnelTable entry, status is tunnelUp

3.5.2 Failover Traps

Table 3.7 Guide to Failover Traps

Trap OID and Definition	Severity	(When Cleared) Traps Received	(When Cleared) Polling Information
failoverSubnetFailoverTrap User Group Failover occurred.	clear	N/A	N/A
failoverSubnetFailbackTrap User Group Failback succeeded.	clear	N/A	N/A
failoverSubnetFailTrap User Group Failover failed because no backup was available.	major	failoverSubnetFailover	N/A
failoverBackChanTimeoutTrap Redundant Hardware Back-channel communication problem.	minor	failoverHardwareClear	N/A
failoverHeartbeatTimeout Redundant Hardware missed heartbeat messages.	minor	failoverHardwareClear	N/A
failoverLinkIntegTrap Redundant Hardware link integrity problem.	minor	failoverHardwareClear	N/A
failoverTakeoverTrap Redundant Hardware takeover has been completed successfully.	info	N/A	N/A
failoverHardwareClear	clear	N/A	N/A

Trap OID and Definition	Severity	(When Cleared) Traps Received	(When Cleared) Polling Information
This clears redundant hardware failover alarms: failoverBackChanTimeoutTrap, failoverHeartbeatTimeoutTrap, and failoverLinkIntegTrap.			

3.5.3 Corente SCP Traps

Table 3.8 Guide to Corente SCP Traps

Trap OID and Definition	Severity	(When Cleared) Traps Received	(When Cleared) Polling Information
ncpTunDownTrap Tunnel between Corente SCP and Location gateway is down.	minor	ncpTunUpTrap	N/A
ncpTunUpTrap Tunnel between Corente SCP and Location gateway is up.	clear	N/A	N/A

3.5.4 Partner Traps

Table 3.9 Guide to Partner Traps

Trap OID and Definition	Severity	(When Cleared) Traps Received	(When Cleared) Polling Information
partnerDownTrap Tunnel to buddy is down and not yet started.	major	partnerUpTrap	tunnelTable entry, status is tunnelUP
partnerUpTrap Tunnel between Location gateway and its partner is up..	clear	N/A	N/A

3.5.5 Security Traps

Table 3.10 Guide to Security Traps

Trap OID and Definition	Severity	(When Cleared) Traps Received	(When Cleared) Polling Information
securityHndShkFailTrap Special digital handshake failed validation.	major	N/A	tunnelTable entry, status is tunnelUP

Trap OID and Definition	Severity	(When Cleared) Traps Received	(When Cleared) Polling Information
securityHsDsvFailTrap Corrupted or hijacked key, bad digital signature, or violated message.	major	securityTunClearTrap	tunnelTable entry, status is tunnelUP
securityHsIdFailTrap Self-verifying information does not match expected sender.	major	securityTunClearTrap	tunnelTable entry, status is tunnelUP
securityHsChpFailTrap Wrong challenge response or returned message.	major	securityTunClearTrap	tunnelTable entry, status is tunnelUP
securityHsMdsFailTrap Message missing digital signature.	major	securityTunClearTrap	tunnelTable entry, status is tunnelUP
securityHsCmdFailTrap Possible corrupted message received from partner has unknown message type.	major	securityTunClearTrap	tunnelTable entry, status is tunnelUP
securityHsOutFailTrap Message sequence from partner is out-of-order.	major	securityTunClearTrap	tunnelTable entry, status is tunnelUP
securityOrgMultConnTrap Network device attempted to contact Location gateway as a partner that already has an active session.	info	N/A	N/A
securityTunClearTrap This clears the tunnel security alarm identified by the partnerFullname.	clear	N/A	N/A

3.5.6 Software Error Traps

Table 3.11 Guide to Software Error Traps

Trap OID and Definition	Severity	(When Cleared) Traps Received	(When Cleared) Polling Information
swErrorInvAclTrap Internal error detected while processing a local User Group tree.	major	swErrorClearTrap	N/A
swErrorInvRmtAclTrap Internal error detected while processing a remote User Group tree.	major	swErrorTunClearTrap	tunnelTable entry, status is tunnelUP

Trap OID and Definition	Severity	(When Cleared) Traps Received	(When Cleared) Polling Information
swErrorIntErrTrap Internal processing error.	minor	swErrorClearTrap	N/A
swErrorClearTrap Internal processing error alarm trap is cleared.	clear	N/A	N/A
swErrorTunClearTrap User Group processing error alarm trap has been cleared.	clear	N/A	N/A

3.5.7 General Traps

Table 3.12 Guide to General Traps

Trap OID and Definition	Severity	(When Cleared) Traps Received	(When Cleared) Polling Information
shutdownStartTrap Corente Services Gateway shutdown process has just started.	info	N/A	N/A
upgradeStartTrap The automatic software upgrade process has just started.	info	N/A	N/A
upgradeSuccessTrap The Corente Services Gateway software upgrade has completed successfully.	clear	N/A	N/A
upgradeFailTrap Automatic software upgrade has failed.	critical	upgradeSuccessTrap	N/A
nsNotifyShutdown An indication that the agent is in the process of being shut down.	info	N/A	N/A
coldStart The SNMP entity, supporting a notification originator application, is reinitializing itself and that its configuration may have been altered.	info	N/A	N/A

3.5.8 Application Monitoring Traps

Table 3.13 Guide to Application Monitoring Traps

Trap OID and Definition	Severity	(When Cleared) Traps Received	(When Cleared) Polling Information
appmonConfigTrap There is a problem with the configuration of application monitoring.	major	appmonAppSvcUpTrap, appmonAppSvcDownTrap, appmonAppSvcUnknownTrap, appmonAppSvcWarnTrap, appmonClearConfigTrap	N/A
appmonAppSvcUpTrap Application service is up.	clear	N/A	N/A
appmonAppSvcDownTrap Application service is down.	major	appmonAppSvcUpTrap	N/A
appmonAppSvcUnknownTrap The status of the application service is unknown.	minor	appmonAppSvcUpTrap	N/A
appmonAppSvcWarnTrap The status of the application service is warning.	minor	appmonAppSvcUpTrap	N/A
appmonClearConfigTrap This clears the configuration alarm identified by appmonConfigTrap.	clear	N/A	N/A

The Corente Services Gateway attempts to notify its trap listeners every 15 minutes if some service affecting alarms stay un-cleared. These repeated alarms are:

- configOpen551Trap
- configSubnetCnfTrap
- configNatPolicyTrap
- configNoInbSpaceTrap
- configNoMagSpaceTrap
- configNatPrhbtTrap
- configAddrCnfTrap
- configAddrNestedTrap
- configAddrCmmtdTrap
- configInbAddrCntTrap
- configDhcpTailTrap
- configRasCnfTrap

- configLclAddrCnfTrap
- configTubeFailTrap
- configNoNatExtLinkTrap
- failoverSubnetFailTrap
- ncpTunDownTrap
- partnerDownTrap
- securityHndShkFailTrap
- securityHsDsvFailTrap
- securityHsIdFailTrap
- securityHsChpFailTrap
- securityHsMdsFailTrap
- securityHsCmdFailTrap
- securityHsOutFailTrap
- swErrorLclAclTrap
- swErrorInvRmtAclTrap
- swErrorIntErrTrap
- appmonConfigTrap
- appmonAppSvcDownTrap

Chapter 4 Using Network Address Translation (NAT)

Table of Contents

When connecting locations for your application network, overlapping IP addresses will create a problem. If two networks in different locations contain IP addresses in the same address space, packets will not get routed to the appropriate computers. The typical solution is to manually remap one of the networks into a different address space. This approach is cumbersome and may be impossible if you are attempting to connect to the network of another company that is imported into your application network with an extranet.

Network Address Translation (NAT) can be used to solve this problem. NAT allows for better organization of the application network and allows locations with overlapping IP address space to establish tunnels with little manual intervention. Corente Cloud Services Exchange provides the following NAT solutions for each Corente Services Gateway that are enabled on the Location form:

- Outbound NAT (User Groups tab)
- Inbound NAT (Partners tab)
- Auto Resolve NAT (Partners tab)

These NAT solutions all assign a specific IP address to each computer so that each machine will appear as a unique NATed address to other computers. This is unlike Internet Connection Sharing (ICS), in which many machines appear as one IP address.

4.1 Outbound NAT

In the App Net Manager, Outbound NAT is enabled on the User Groups tab on a per address range basis in the Default User Group. The address range will be NATed to a specified range of addresses for all partners of this Location gateway. Outbound NAT translates a local subnet of IP addresses to another subnet before the subnet is made visible to remote application network partners.

The Specified setting of Outbound NAT is a useful way of organizing an entire application network. An administrator can map each User Group in the application network to a distinct set of address ranges so that there are no address conflicts. The traffic from each site can then be identified by the range into which it was mapped. It is the administrator's responsibility to guarantee that there are no conflicts between the addresses that are specified for each subnet.

The primary use of the Prohibited setting of Outbound NAT is to prevent NATing on a connection that is transporting a protocol containing embedded IP addresses, such as FTP. This type of protocol will not work correctly through a NATed connection. Prohibited will prevent any NATing by a Location partner (Inbound NAT or Auto Resolve NAT) that would cause a problem.

4.2 Inbound NAT

Inbound NAT is enabled on a per Location partner basis on the Partners tab for each Location partner.

If Inbound NAT is enabled on a Location partner, the Corente Services Gateway will remap the partner's User Group to the subnet that you specify. Unlike Auto Resolve NAT, this setting will remap the addresses even if there are no address conflicts. The NATed IP addresses will only be visible by local computers. The remote computers will not know that they have been NATed.

To solve address direct conflicts between two Location partners, both partners must enable Inbound NAT for each other so that address conflicts are resolved on both sides of the application network connection.

4.3 Auto Resolve NAT

Auto Resolve NAT is enabled on a per partner basis on the Partners tab for each partner. If Auto Resolve NAT is enabled on a Location partner, the Corente Services Gateway will automatically resolve addressing conflicts with the partner by mapping the partner's User Group to a new set of non-conflicting addresses. The NATed IP addresses will only be visible by local computers. The remote computers will not know that they have been NATed.

Auto Resolve NAT is particularly useful for resolving address conflicts between extranet partners, where neither administrator can control both networks nor the address spaces used in those networks.

To resolve overlapping address spaces between Location partners, each side must enable Auto Resolve NAT.

4.4 Indirect Conflicts

Besides correcting direct address conflicts between Location partners, Auto Resolve NAT and Inbound NAT can also be used to correct indirect address conflicts.

Consider the following scenario. In an application network containing three Corente Services Gateways (Miami, Houston, and Nashville), Miami is partners with both Houston and Nashville. Houston and Nashville are not partners with each other.

The User Group of Houston and the User Group of Nashville contain the same subnets. This does not cause a Configuration Alert between them, because they are not partners and therefore do not detect any address conflicts. However, Miami will detect a conflict because it is attempting to connect to both User Groups.

- If Miami enables Inbound NAT for both Houston and Nashville, it will remap the IP addresses to new address spaces and no conflicts will occur.
- If Miami enables Auto Resolve NAT for both Houston and Nashville, it will automatically remap one of the User Groups to a new address space and prevent the conflicts from occurring.

Note that neither Houston nor Nashville have to enable Auto Resolve NAT.

4.5 Perform DNS/WINS Fixup

If you are using DNS or WINS servers on your network for name resolution, it is normally recommended that you do not use the NAT options. DNS and WINS will not work with NAT, unless they are administered using the NAT addresses for name resolution.

However, the Perform DNS/WINS Fixup option allows DNS and WINS to function with NATed subnets. When this option is selected on the Network tab, computers behind the Corente Services Gateway will

always use the correct IP address to connect to another computer across the application network. Either the real IP address or the NATed IP address is used, as appropriate.

4.6 Specifications

The following specifications apply when using Corente Cloud Services Exchange NAT solutions:

- As with any other NAT solution, applications that carry IP addresses in the payload, such as ones that include the IP address for a computer as part of the data inside the packet, will not work. Care must be taken to understand the applications that you are usin,g to ensure that NAT will be able to solve your problem. In particular, the H.323 (Netmeeting) protocol will not work with NAT.

  However, a fixup module is included that allows active FTP over NATed connections. Active FTP is usually forbidden on NATed subnets.

- NAT will not function correctly for Corente Clients, because these clients are bridged directly to the Location gateway's LAN.

Chapter 5 Securing Your LAN with a Demilitarized Zone (DMZ)

Table of Contents

In networking, the demilitarized zone (DMZ) is a buffer between the private LAN and the public Internet or WAN. Servers that will be accessed both by machines on the private LAN and machines over the Internet/WAN, such as web or mail servers, are often placed in this zone to prevent unwanted traffic from the Internet/WAN from infiltrating the private LAN.

To implement a DMZ with Corente Cloud Services Exchange:

- Your DMZ must consist of a single, fixed-address subnet, configured with private addresses.
- Your Corente Services Gateway must be using an Inline configuration.
- One extra Ethernet card must be installed in the gateway hardware, in addition to the two Ethernet cards required for an Inline configuration. The card must be configured with an IP address on the same private subnet as the DMZ servers.
- If you have multiple servers in the DMZ that will be using the same port numbers to receive traffic, one of these servers can use the WAN address of the gateway to receive traffic, but you must obtain a routable address for each additional server.

Traffic reaches servers on the DMZ via port forwarding from the gateway's WAN interface. To prevent security breaches of your LAN, all traffic to and from the DMZ is denied unless explicitly permitted in App Net Manager.

5.1 Port Forwarding and Alias Addresses

Normally, a Corente Services Gateway prevents access to the LAN from the Internet/WAN, allowing external connections only from partner Locations or Corente Clients. Sometimes, however, your corporate network contains servers that must be reachable by Internet/WAN traffic. For example, a web server that serves your company's website, or a mail server that must be reachable by other mail servers so that your employees can get emails from outside your company. Despite the fact that these servers should remain inside your LAN or DMZ so that they are protected and cannot be compromised by external attacks, they require a public address so that they are reachable by computers on the Internet/WAN when contacted with the permitted type of traffic. Port forwarding allows these servers to use the gateway's WAN interface as their own public interface, with the gateway filtering out the unwanted traffic and passing on only the approved type of traffic to the designated server.

Specifically, port forwarding allows an administrator to forward traffic bound for particular ports of the gateway's WAN address to the appropriate servers behind the gateway. For example, port forwarding can be configured so that all traffic pointed at the gateway's WAN address and port 80 (the standard port used for HTTP traffic) is forwarded by the gateway to a web server in your DMZ. Your web server is secured safely behind the gateway yet still reachable from the Internet/WAN; the LAN addressing is hidden and the gateway makes certain that only the traffic you choose to allow can reach the server.

In addition, if multiple DMZ servers will need to utilize the same port, an administrator can create multiple alias addresses for the gateway's WAN interface and ensure that all incoming traffic through the gateway to that alias address is forwarded to specific servers on the private LAN of the DMZ. Aliases are used, for example, when you have two web servers in your DMZ that both use HTTP on port 80. One server can use the WAN address of the gateway as its routable address, but each additional server using port 80 will require a distinct routable address to ensure that traffic is routed appropriately. The addresses that you use as aliases must be routable addresses that are otherwise not in use.

Port forwarding and aliases are not necessarily used only with a DMZ; they can also be used whenever you have multiple servers using the same port and you would like them all to be reachable from the Internet/WAN. These multiple servers may not reside in your DMZ, but directly on your LAN.

5.2 Implement a DMZ with Corente Cloud Services Exchange

Corente Cloud Services Exchange provides two DMZ configurations:

- **Typical DMZ Configuration**

  In the most typical DMZ configuration, servers residing in the DMZ each use a single Ethernet interface that is configured on a private subnet. All traffic to and from the DMZ, between the DMZ and both the LAN and the Internet/WAN, is managed by the Corente Services Gateway.

- **Alternate DMZ Configurations**

  There are two other possible DMZ configurations, both of which require two Ethernet interfaces on each server in the DMZ: one interface is on the same private subnet as the Corente Services Gateway's DMZ interface, and the other interface is on either the LAN side of the DMZ or the Internet/WAN side of the DMZ.

  - When the additional interface is on the LAN side of the DMZ, the gateway will handle security only for traffic between the Internet/WAN and the DMZ.

    The DMZ to Internet Access partner is used. You should not configure the LAN to DMZ Access partner.

  - When the additional interface is on the Internet/WAN side of the DMZ, the Corente Services Gateway will handle security only for traffic between the LAN and the DMZ.

    The LAN to DMZ Access partner is used. You should not configure the DMZ to Internet Access partner.

  This means that, for both alternate configurations, you must supply your own security measures for the side that is not being protected by the gateway.

5.3 Example DMZ Configuration

This section reviews the basic considerations to keep in mind when designing your DMZ and configuring it in App Net Manager.

For example, if you have two web servers and a mail server on your corporate network. These servers must be accessed both by machines on the LAN and machines on the Internet/WAN, so you would like them to reside separately from your corporate network to ensure that outside machines do not use these servers to launch intrusion attacks.

Create a DMZ by setting up a private subnet on your LAN consisting of only these three servers. On your Corente Services Gateway, set up an Ethernet interface that also resides on this private subnet. Register at least one alias for the gateway's WAN interface that can be used for one of the web servers.

Configure a Default User Group – DMZ on your gateway in App Net Manager that includes the private subnet on which the mail server and web servers reside. For web traffic, register an HTTP application on the Applications tab for each web server Using the web server private IP addresses. For mail traffic, register two mail server applications on the Applications tab using the mail server's private address. One application must allow POP traffic, and the other application must allows SMTP traffic.

To control access to the DMZ, edit your Firewall Policies and the DMZ to Internet Access and LAN to DMZ Access partners on the Partners tab of the gateway's Location form.

- The DMZ to Internet Access partner should have at least three tubes: one for the first web server application via the WAN interface of the gateway, one for the second web server application via the alias address, and one for the SMTP mail server application via the WAN interface of the gateway.
- The LAN to DMZ Access partner can have a more simple configuration and still maintain security. You can create a tube that allows the entire LAN to access the entire Default User Group – DMZ, with a Firewall Policy that allows all traffic from the LAN to the DMZ but denies all traffic from the DMZ to the LAN. Note that a Firewall Policy defines who is allowed to initiate a connection, but all return traffic from the connection is always allowed.

If you would like to create a more definite set of permissions, this partner should have as many tubes as needed to access and control the DMZ servers. There should be at least three tubes: one for the first web server application, one for the second web server application, and one for the POP mail server application. You may also want to create a tube that allows the type of traffic needed to maintain and update all the DMZ servers from the LAN, using the Default User Group – DMZ and a Firewall Policy that allows only the type of traffic used to maintain and update the servers.

5.4 Partner Access to the DMZ

If you would like to allow Corente Clients or computers at partner Locations to access machines on the DMZ as if they were local computers, ensure that at least one User Group, or the entire Default User Group – DMZ itself, is within the secure network. Use the User Group is Within Secure Network option on the User Groups tab. Then, create tubes from the Corente Client or Location partner to that User Group.

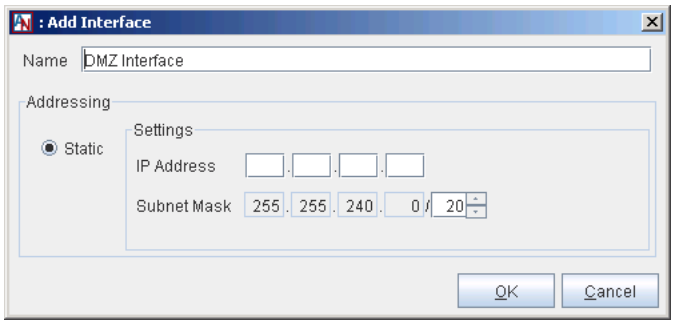
5.5 Configure the DMZ Interface

After physically setting up the DMZ subnet and assigning IP addresses to the servers, personality file configuration for the Corente Services Gateway that is supporting the DMZ begins on the Network tab of the gateway's Location form in App Net Manager. Use this tab to register the Ethernet interface of the gateway that will connect to the DMZ.

To access this tab, right-click the gateway's name and select Edit. The Location form will be displayed. Click Network from the tabs across the top of this form. In the Network Interfaces section of this tab, you must click the Add button to register the DMZ interface.

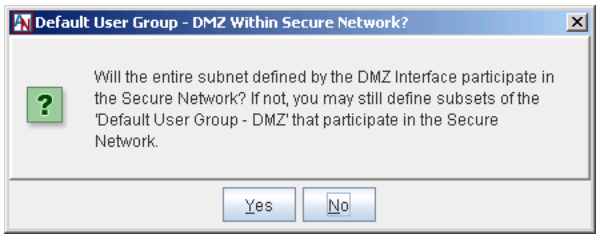
On the window that is displayed, select DMZ Interface and click OK. The Add Interface window will be displayed.

Figure 5.1 Add Interface



Supply an IP address and subnet mask for the gateway's DMZ interface. Remember that this address must be on the same private subnet as the servers in the DMZ. Click OK. When you select OK, a series of dialog boxes will be displayed that allow you to perform several automatic personality configurations.

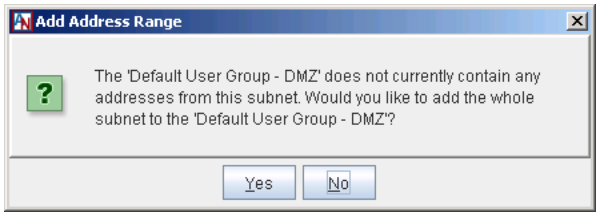
Figure 5.2 Add Interface



In the first dialog box, if you select Yes, by default, the entire DMZ subnet will be available to share across the secure Corente Services network with the Corente Services Gateway partners. Computers at partner Locations can be permitted to access servers on the DMZ in the same way that computers on the LAN access them.

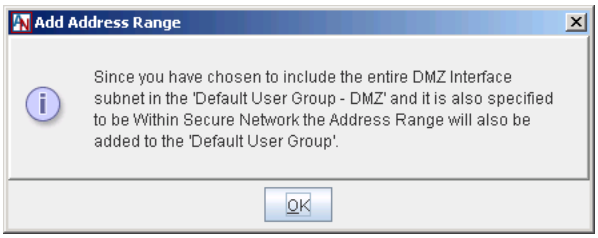
If you select No, by default, the entire DMZ subnet will not be shared over the Corente Services network. Computers at partner Locations must connect to servers on the DMZ like machines from the Internet/WAN. If you select No, you can later define subsets of the subnet that will be included in the secure network on the User Groups tab of the Location form.

Figure 5.3 Add Address Range



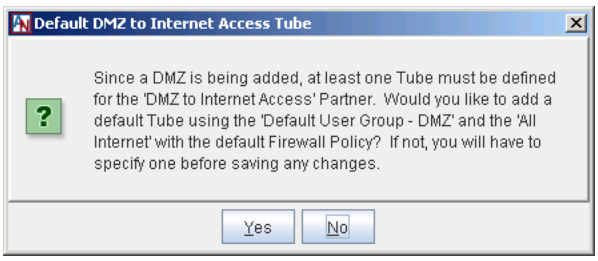
When adding the DMZ interface, a new User Group is created on the User Groups tab of the Location form: the Default User Group – DMZ. The creation of this default User Group informs the Corente Services Gateway what particular sets of addresses are participating in the DMZ. If you select Yes in this dialog box, you will populate the Default User Group – DMZ with the entire subnet in which the DMZ exists. If you select No, the User Group will be created, but will be empty, and you must populate the group manually on the User Groups tab.

Figure 5.4 Add Address Range Note



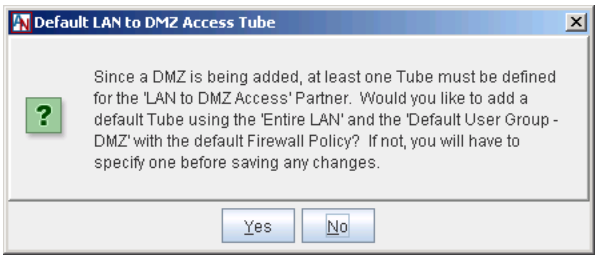
If you selected Yes for the both of the previous dialog boxes, a third dialog box will be displayed to inform you that the DMZ subnet will be added to the main Default User Group for the gateway. The Default User Group contains all addresses on the LAN that are permitted to participate in the secure Corente Services network.

Figure 5.5 Default DMZ to Internet Access Tube



The next dialog box enables you to automatically create a tube on the Partners tab for the DMZ to Internet Access partner that allows all machines on the Internet to connect to the Default User Group – DMZ using the default DMZ to Internet Firewall Policy for your domain. By default, this firewall policy denies all inbound and outbound traffic. You will be able to modify this tube and add new tubes for the DMZ to Internet Access partner at any time. If you select No, no tube will be created, so you must manually create this tube on the Partners tab.

Figure 5.6 Default LAN to DMZ Access Tube



The final dialog box enables you to automatically create a tube on the Partners tab for the LAN to DMZ Access partner that allows any machine on the LAN to connect to the Default User Group – DMZ using the default LAN to DMZ Firewall Policy for your domain. By default, this firewall policy denies all inbound and outbound traffic between the LAN and the DMZ. You will be able to modify this tube and add new tubes for the LAN to DMZ Access partner at any time. If you select No, no tube will be created, so you must manually create this tube on the Partners tab.

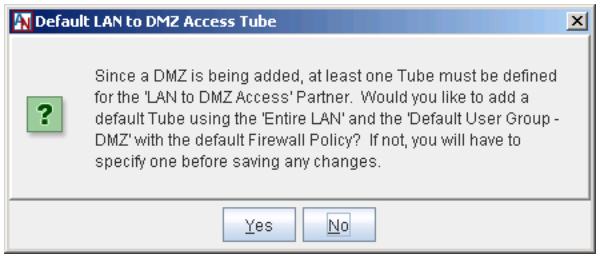
5.6 Configure Alias Addresses for the WAN Interface

After registering the Corente Services Gateway's DMZ interface, you might need to create alias addresses for the WAN interface. Begin by obtaining as many routable addresses as you will need for your particular configuration.

5.7 Configure the Default User Group - DMZ

When you add a DMZ Interface on the Network tab, the Default User Group – DMZ is automatically created on the User Groups tab. To define or change the definition of this User Group, select the group and click Edit.

Figure 5.7 Edit Default User Group – DMZ



The Edit Default User Group – DMZ screen will be displayed. Fill out the fields as follows:

User Group Name: This name will be Default User Group – DMZ by default and cannot be changed.

Firewall Policy: Choose a Firewall Policy from those that you have defined for your domain from the pull-down menu to enable this policy for all traffic inbound to and outbound from all of the machines within the Default User Group – DMZ.

Outbound QoS: Choose a QoS entry from those that you have defined for your domain from the pull-down menu to enable the entry for all traffic outbound from the machines within the Default User Group – DMZ.

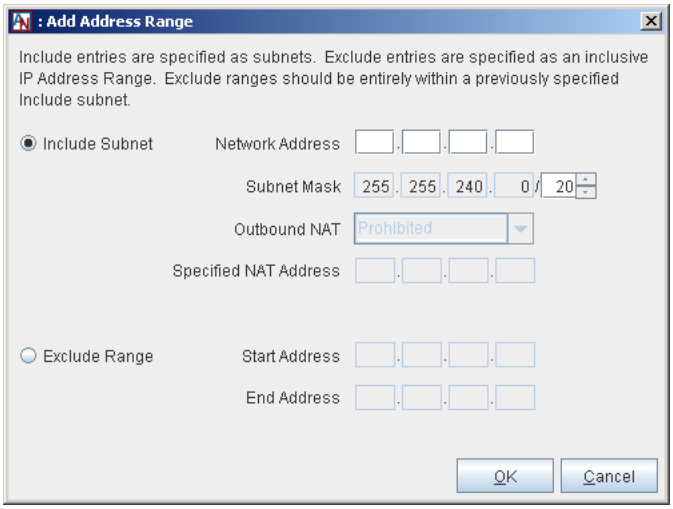
Inbound QoS: Choose a QoS entry from those that you have defined for your domain from the pull-down menu to enable the entry for all traffic inbound to the machines within the Default User Group – DMZ.

User Group is Within Secure Network: This selection will either be selected or deselected based upon your choice in the DMZ Within Secure Network? dialog box that was shown when you enabled the DMZ Interface on the Network tab, and cannot be changed. If this box is selected, all of the members of this User Group will be available to share as local machines with partners across the Corente Services network.

Special Internal Network Description User Group: This option is unavailable.

User Group Subnets/Address Ranges: If you used the Add Address Range dialog box to add the entire DMZ subnet to the Default User Group – DMZ, then this table will be prepopulated with an entry containing the entire DMZ subnet. You can edit any entries by selecting the entry and then selecting the Edit button, delete entries by selecting the entry and then selecting the Delete button, or add address ranges to this table by clicking the Add button.

Figure 5.8 Add Address Range



On the Add Address Range screen that is displayed when you select Add, begin by selecting whether you will be Including an entirely new subnet within the Default User Group – DMZ or Excluding an address range from a previously included subnet.

- If you are *Including* a subnet, enter the following:
  - **Network Address:** The IP address of the subnet.
  - **Specified NAT Address:** This option is unavailable.
  - **Subnet Mask:** The network mask for the subnet.
  - **Outbound NAT:** This option is unavailable.
- If you are **Excluding** an address range, enter the following:
  - **Start Address:** The first IP address in the range.
  - **End Address:** The last IP address in the range.

Click OK to add the Include or Exclude to the Default User Group – DMZ definition.

When you are finished defining the Default User Group – DMZ, click OK to save your changes.

If your Default User Group – DMZ is not participating in the secure Corente Services network, you can define subsets of the User Group that are included in the secure network and that can be shared with partners. Add a new User Group containing DMZ addresses, with the User Group is Within Secure Network option selected.

To refine access permissions, you can create additional User Groups that are subsets of the Default User Group – DMZ and you can register applications provided by DMZ servers on the Applications tab of the Location form. These additional User Groups and applications can be used to create tubes that define specific access permissions.

5.8 Configure Access to the DMZ on the Partners Tab

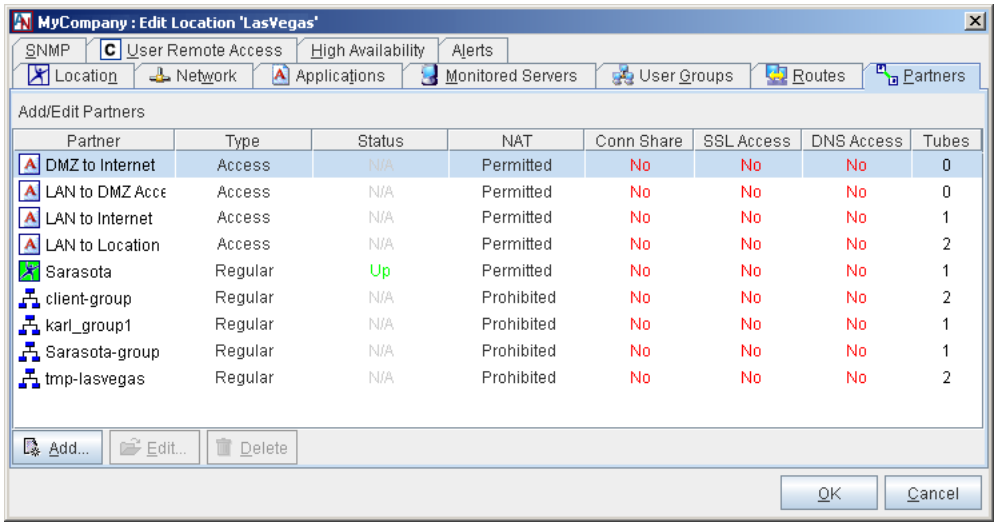
Configuring access to the DMZ takes place on the Partners tab of the Location form, using two partner configurations. DMZ to Internet Access controls traffic between computers on the Internet/WAN and the DMZ, and LAN to DMZ Access controls traffic between computers on your LAN and the DMZ.

By default, to protect the LAN, the default Firewall Policies for these partners are set to deny all traffic. Your DMZ configuration must explicitly allow traffic to enter and leave the DMZ. Before accessing the Partners tab, ensure that the DMZ to Internet and LAN to DMZ Firewall Policies, or any other Firewall Policies that you will be using, are configured to allow the correct traffic to traverse the firewall.

Note

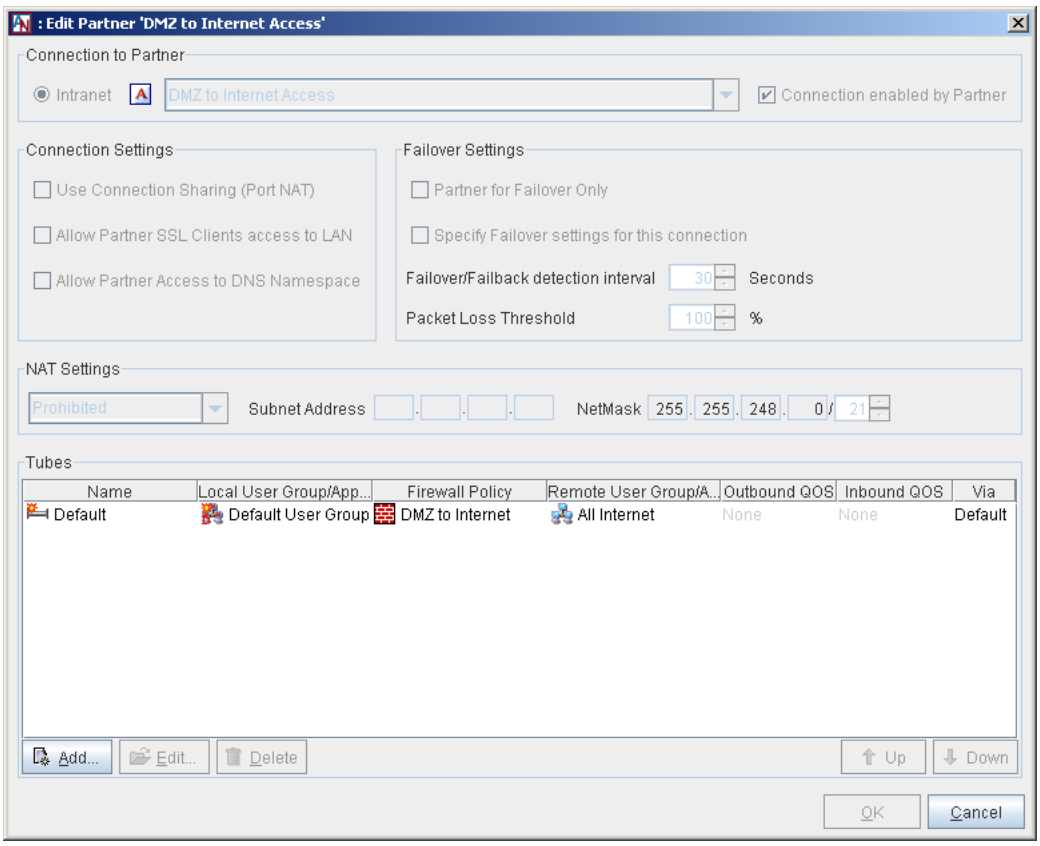
- If the gateway is providing security only between the Internet and the DMZ, you only need to configure the **DMZ to Internet Access** partner.
- If the gateway is providing security only between the DMZ and the LAN, you only need to configure the **LAN to DMZ Access** partner.

Figure 5.9 Partners Tab



To edit the DMZ to Internet Access or LAN to DMZ Access partner, select the partner and click Edit.

Figure 5.10 Partners Tab



On the Edit Partner screen that is displayed, you will only have the ability to create, edit, and delete tubes. If you selected Yes on the Default DMZ to Internet Access Tube dialog box when first enabling your DMZ interface on the Network tab, by default, a tube will be defined for the DMZ to Internet Access partner that permits traffic between the Internet and the entire Default User Group – DMZ using the DMZ to Internet Firewall Policy.

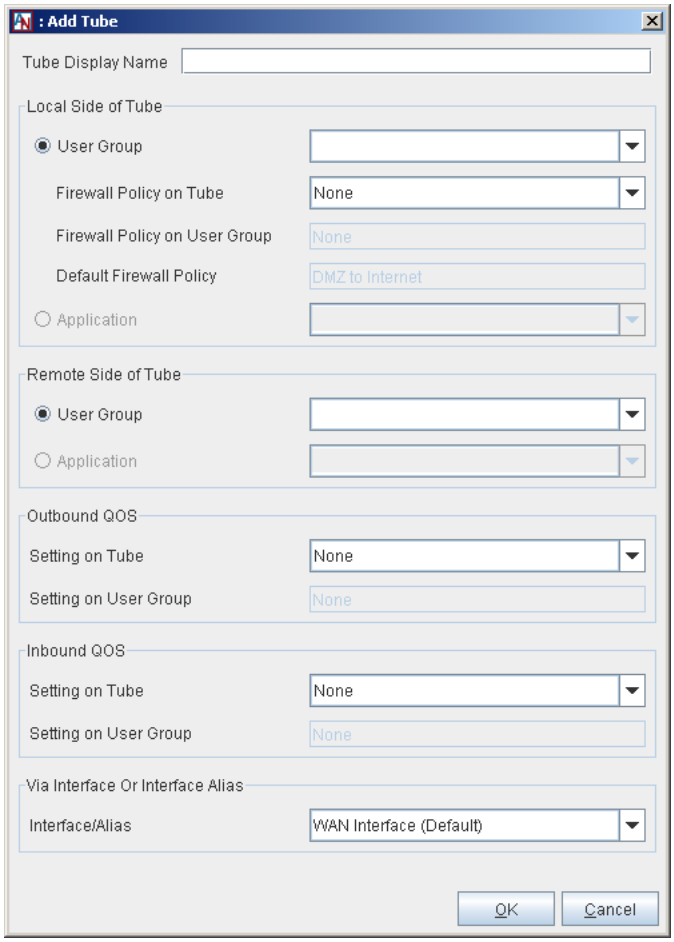
Similarly, if you selected Yes on the LAN to DMZ Access Tube dialog box when first enabling your DMZ interface, a tube will be defined for the LAN to DMZ Access partner that permits traffic between the LAN and the entire Default User Group – DMZ using the LAN to DMZ Firewall Policy.

You can edit these tubes or add new tubes to refine DMZ permissions.

For either access partner, to add a new tube, click Add. The Add Tube screen will be displayed.

5.8.1 DMZ to Internet Access Tubes

Figure 5.11 DMZ to Internet Access Tube



On this screen, create a tube for the DMZ to Internet Access partner as follows:

Tube Display Name: (Optional) Enter a name for the tube in this field.

Local Side of Tube: This section defines the local side of the tube.

- **User Group:** Select User Group if you would like a local User Group to participate in this tube. Choose the User Group from the adjacent pull-down menu. Only those User Groups that are within the DMZ will be available for selection.

  When the User Group option is selected, you can define what traffic you will allow to enter and leave between the DMZ User Group and the Internet. The following Firewall Policy option is available:

  - **Firewall Policy on Tube:** Select a Firewall Policy that you would like to apply to traffic traveling between this User Group and the Internet.

    Below this option are the following additional fields:

    - **Firewall Policy on User Group:** If there is a Firewall Policy that was enabled when defining the selected User Group and always applies to this User Group, the Firewall Policy will be displayed in this field.

    - **Default Firewall Policy:** The default firewall policy for this type of connection will be displayed in this field. For example, DMZ to Internet.

All three Firewall Policies are listed here to remind you that Firewall Policies will be enforced on the connection in this order: Tube Firewall Policy, User Group Firewall Policy, and then Default Firewall Policy.

- **Application:** Select Application if you would like a local application to participate in this tube. Choose the application from the adjacent pull-down menu. Only those applications whose servers are in the DMZ (in other words, their server IP addresses fall within the address ranges of the Default User Group – DMZ) will be available for selection.

Remote Side of Tube: This section defines the remote side of the tube. For a DMZ to Internet Access tube, the remote side is either the Internet or local User Groups/applications that are not participating in the Corente Services network.

- **User Group:** Select User Group if you would like a remote User Group to participate in this tube. The pulldown menu will list two kinds of User Groups: an "All Internet" User Group and local User Groups that are defined for this Location that are not participating in the secure Corente Services network.

- **Application:** Select Application if you would like a remote application to participate in this tube. The pulldown menu will list only those local applications defined for this Location that are not participating in the secure network and that are not served from servers residing in the DMZ (as defined by the Default User Group – DMZ).

Outbound QoS: This section enables you to configure Quality of Service (QoS) settings for the outbound traffic on this tube. For example, traffic from the DMZ to the Internet. QoS settings are viewable and configurable with the Quality of Service feature in App Net Manager.

- **Setting on Tube:** Choose a QoS entry from the pull-down menu to specify the priority of traffic outbound on this tube.

Note

As when performing any sort of QoS configuration, administrators must be careful when assigning QoS levels because if there is too much high priority traffic, any other traffic with a lower level of priority may become too slow or even be dropped. In addition, you cannot use QoS to prioritize traffic to or from a Corente Client.

- **Setting on User Group:** If there is an Outbound QoS Setting that was enabled when defining the selected User Group or Application and always applies to this User Group or Application, the Outbound QoS Setting will be displayed in this field. This field is displayed to remind you that QoS settings will be enforced on the connection in this order: Tube QoS setting and then User Group QoS setting.

Inbound QoS: This section enables you to configure QoS settings for the inbound traffic on this tube, such as traffic to the DMZ from the Internet.

- **Setting on Tube:** Choose a QoS entry from the pull-down menu to specify the priority of traffic inbound on this tube.

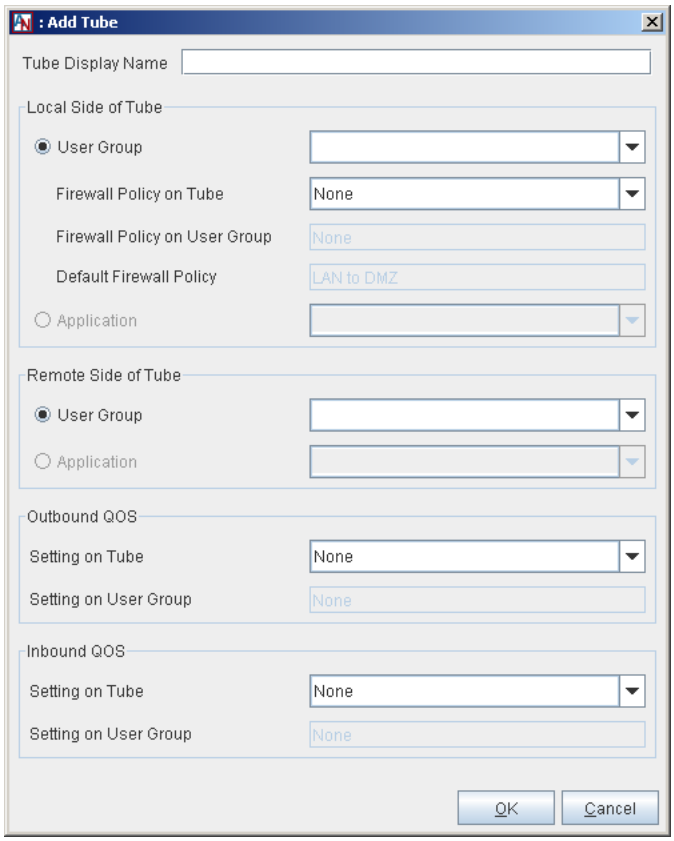
- **Setting on User Group:** If there is an Inbound QoS Setting that was enabled when defining the selected User Group/application and always applies to this User Group/application, the Inbound QoS Setting will be displayed in this field. This field is displayed to remind you that QoS settings will be enforced on the connection in this order: Tube QoS setting and then User Group QoS setting.

Via Interface or Interface Alias: Choose the WAN interface or a WAN interface alias from the Interface/Alias pull-down menu. This will enforce the rules of this tube only for traffic that is destined for the interface or address that you have chosen. If necessary, you can create alias addresses on the Network tab.

When you have finished defining the tube, select OK to store your changes or Cancel to close the screen and discard your changes. The new tube will appear in the Tubes table.

5.8.2 LAN to DMZ Access Tubes

Figure 5.12 LAN to DMZ Access Tube



On this screen, create a tube for the LAN to DMZ Access partner as follows:

Tube Display Name: If you would like, enter a name for the tube in this field.

Local Side of Tube: This section defines the local side of the tube.

- **User Group:** Select User Group if you would like a local User Group to participate in this tube. Choose the User Group from the adjacent pull-down menu, which will list all local User Groups that have been defined for the LAN. In other words, all non-DMZ User Groups.

  When the User Group option is selected, you can define what traffic you will allow to enter and leave your LAN between the local side and the DMZ. The following Firewall Policy option is enabled:

  - **Firewall Policy on Tube:** Select a Firewall Policy that you would like to apply to traffic traveling between this User Group and the DMZ.

    Below this option are the following additional fields:

    - **Firewall Policy on User Group:** If there is a Firewall Policy that was enabled when defining the selected User Group and always applies to this User Group, the Firewall Policy will be displayed in this field.

- **Default Firewall Policy:** The default firewall policy for this type of connection will be displayed in this field. For example, LAN to DMZ.

All three Firewall Policies are listed here to remind you that Firewall Policies will be enforced on the connection in this order: Tube Firewall Policy, User Group Firewall Policy, and then Default Firewall Policy.

- **Application:** Select Application if you would like a local application to participate in this tube. Choose the application from the adjacent pull-down menu, which will list all local applications that have been defined for the LAN. In other words, all non-DMZ applications.

Remote Side of Tube: This section defines the remote side of the tube (the DMZ).

- **User Group:** Select User Group if you would like a DMZ User Group to participate in this tube. The pulldown menu will list the Default User Group – DMZ as well as any User Groups you have defined that contain addresses within the DMZ.

- **Application:** Select Application if you would like a remote application to participate in this tube. Choose the application from the adjacent pull-down menu. Only those applications whose servers are in the DMZ are available for selection. In other words, their server IP addresses fall within the address ranges of the Default User Group – DMZ.

Outbound QoS: This section enables you to configure Quality of Service (QoS) settings to the outbound traffic on this tube.

- **Setting on Tube:** Choose a QoS entry from the pull-down menu to specify the priority of traffic outbound from the LAN on this tube.

- **Setting on User Group:** If there is an Outbound QoS Setting that was enabled when defining the selected User Group/application and always applies to this User Group/application, the Outbound QoS Setting will be displayed in this field. This field is displayed to remind you that QoS settings will be enforced on the connection in this order: Tube QoS setting and then User Group QoS setting.

Inbound QoS: This section enables you to configure QoS settings to the inbound traffic on this tube.

- **Setting on Tube:** Choose a QoS entry from the pull-down menu to specify the priority of traffic inbound from the LAN on this tube.

- **Setting on User Group:** If there is an Inbound QoS Setting that was enabled when defining the selected User Group or Application and always applies to this User Group or Application, the Inbound QoS Setting will be displayed in this field. This field is displayed to remind you that QoS settings will be enforced on the connection in this order: Tube QoS setting and then User Group QoS setting.

When you have finished defining the tube, select OK to store your changes or Cancel to close the screen and discard your changes. The new tube will appear in the Tubes table.

Chapter 6 Troubleshooting Corente Cloud Services Exchange

Table of Contents

Troubleshooting Corente Cloud Services Exchange involves following procedures to diagnose and resolve common issues. If you encounter issues with Corente Cloud Services Exchange you should complete the troubleshooting procedures before contacting Oracle Support.

6.1 Getting Started with Troubleshooting

You should begin troubleshooting issues with Corente Cloud Services Exchange by checking the status of your Locations in App Net Manager.

Do the following:

1. Log in to App Net Manager.
2. Expand the **Locations** folder in the domain directory.
3. Select the Location that you need to troubleshoot.

App Net Manager displays a detailed view of the Location. This view is displayed as **Partners of** ***`Location`*** to the right of the domain directory. You can view the status of the Location as well as the tunnels between other Locations. Icons indicate the status of the Location and colored lines indicate the status of each tunnel.

You should identify the status of the Location and each tunnel and then take the appropriate action, as described in the following tables:

Table 6.1 Location Icons

Location Icon	Meaning	Explanation	Action
	Alarm	A yellow triangle on the lower right side of an icon indicates that the Corente Services Gateway is generating an alarm. This feature appears in conjunction with a red or black icon, indicating an alarm has been generated based upon the Corente Services Gateway status.	You can view the active alarms being generated by a Corente Services Gateway by right-clicking the Corente Services Gateway icon and highlighting **Alarms** in the menu that appears. Select an alarm number to view the details of that active alarm, which will indicate what sort of problem the Corente Services Gateway is experiencing. This problem is also indicated by the color of the icon or tunnel, but often the alarm notification

Location Icon	Meaning	Explanation	Action
			will pinpoint a specific connectivity or policy issue to troubleshoot.
	Disconnected	A red square indicates that the Corente Services Gateway has suddenly become disconnected from the SCP, without being powered off safely.	Do the following: a. Ensure the Corente Services Gateway is powered on and that the service has started running. b. Ensure that all Ethernet cables are plugged in and that the indicator lights on the network interfaces are flashing to show that they are active. If the network interfaces do not indicate that they are active, you should replace the cables between the Corente Services Gateway and the Internet Access Device (IAD) and between the Corente Services Gateway and the LAN, if appropriate.
	Inactive	A yellow square indicates that the Corente Services Gateway is currently inactive on the Corente Services network, but has been powered off or is being rebooted safely.	Do the following: a. Ensure the Corente Services Gateway is powered on and that the service has started running. b. Ensure that all Ethernet cables are plugged in and that the indicator lights on the network interfaces are flashing to show that they are active. If the network interfaces do not indicate that they are active, you should replace the cables between the Corente Services Gateway and the IAD and between the Corente Services Gateway and the LAN, if appropriate.
	Denied	A black square indicates that this site is invalid. The Corente Services Gateway at this site will be unable to connect to the SCP.	If the Corente Services Gateway is denied, contact Oracle Support in order to determine the reason.
	Firewalled	A white square with a circular red border means that the Corente Services Gateway appears to be operating behind a firewall that restricts access to TCP port 551.	Any third-party firewall devices between the Internet and the Corente Services Gateway must have port 551 opened to allow both inbound and outbound connections to/from the Corente Services Gateway or the service will not be able to function.

Location Icon	Meaning	Explanation	Action
	Active	A green square indicates that the Corente Services Gateway is functional and has a secure connection with the SCP. It is currently active on the Corente Services network.	• If users are experiencing connectivity issues, you should evaluate policy provisioning for the affected users. • If users are experiencing slow or degraded performance, you should troubleshoot performance issues.

Table 6.2 Tunnel Colors

Tunnel Color	Meaning	Explanation	Action
	Alert	A red line indicates that a problem has occurred with the tunnel.	Do the following: a. Ensure the Corente Services Gateway is powered on and that the service has started running. b. Ensure that all Ethernet cables are plugged in and that the indicator lights on the network interfaces are flashing to show that they are active. If the network interfaces do not indicate that they are active, you should replace the cables between the Corente Services Gateway and the IAD and between the Corente Services Gateway and the LAN, if appropriate.
	Down	A yellow line indicates that the tunnel is down. This is most likely due to the fact that one of the partner Corente Services Gateways is inactive on the Corente Services network, but has been powered off or is being rebooted safely.	Do the following: a. Ensure the Corente Services Gateway is powered on and that the service has started running. b. Ensure that all Ethernet cables are plugged in and that the indicator lights on the network interfaces are flashing to show that they are active. If the network interfaces do not indicate that they are active, you should replace the cables between the Corente Services Gateway and the IAD and between the Corente Services Gateway and the LAN, if appropriate.
	Pending	A pink line indicates that the tunnel is currently in the process of being brought up or being brought down.	You should wait a few minutes to see what color the line becomes before beginning diagnosis. If the color does not change, escalate the issue to Oracle Support for diagnosis.

Tunnel Color	Meaning	Explanation	Action
	Configuration Alert	A black line indicates that the Corente Services Gateway partners are able to communicate with each other. However, the User Groups that each partner is exporting to the other contain conflicting address spaces.	When connecting sites with a Corente Services Gateway, the address ranges used at these sites must not overlap. Unique IP address spaces must be used at each site. To resolve the address conflict, you should use one of the Corente Services NAT options to remap addresses at either site to new addresses for the connection: • **Outbound NAT** is enabled on a local User Group so that when the User Group is made visible to remote partners, the addresses in that User Group are remapped to a specified subnet. • **Inbound NAT** is enabled on a Corente Services Gateway partner so that when the partner's User Group is made visible to the local Corente Services Gateway, the User Group is remapped to a specified subnet. • **Auto Resolve NAT** is enabled between partners so that if the addresses in the User Groups of the partners ever overlap, each range in the User Groups is automatically remapped to another subnet.
	Active	A green line indicates that the tunnel between the site and your hosting center is active.	• If users are experiencing connectivity issues, you should evaluate policy provisioning for the affected users. • If users are experiencing slow or degraded performance, you should troubleshoot performance issues.

6.2 Identifying Connectivity Issues

If you cannot successfully diagnose and resolve issues with Corente Cloud Services Exchange through App Net Manager, you should determine if there is a problem with the Internet Service Provider (ISP) or with the Corente Services Gateway.

You should start troubleshooting a connectivity issue by determining if users who experience the issue can access the Internet. Instruct users to access any external site from their browsers. If the users cannot access the Internet, you should disconnect the Corente Services Gateway and then connect a computer directly to the Internet Access Device (IAD) and try to access the Internet. If you cannot access the Internet, you should contact the relevant ISP to resolve the connectivity issue.

If you can determine that the connectivity issue is not the result of a fault with the ISP, then you should complete the following steps to troubleshoot the Corente Services Gateway:

1. Open the Gateway Viewer.
2. Select **Admin** and then **Admin Login**.
3. Specify the appropriate credentials and then log in.
4. Select **Gateway Admin** and then **Test**.

   The **Test** page provides connectivity information and network tools that help you to identify connectivity issues. Green entries in the **Ping** column indicate active connections.
5. Ensure that there are active connections in the **Domain Name Server** and **Internet** sections, and an active connection to the hub site in the **Partner** section.
6. Select **Traceroute** for any inactive connections.

   The traceroute test identifies where connection issues occur. You can then determine if the connectivity issue is a problem with the ISP or with a specific device on the LAN.

If the **Test** page on the Gateway Viewer does not indicate any problems with the DNS or Internet connections, you should test connectivity to the Corente Services Control Point (SCP). Do the following:

1. Open the Gateway Viewer.
2. Select **Gateway Admin** and then **Test**.
3. Select **Test SCP Connectivity** in the **Network Tools** section.
4. Select **Test Network** to test the Corente SCP connection.
5. Select **Test SCP** on the Corente Gateway Viewer Test Page.

The results of the connection test indicate if the Corente Services Gateway can successfully connect to the Corente SCP through the Internet. If the connection test is not successful, a failure code is displayed to help you diagnose the issue.

6.3 Troubleshooting Policy Provisioning

Occasionally, certain configuration errors in App Net Manager will cause an interruption in service between sites. App Net Manager will alert the user immediately when certain configuration errors are present. However, if App Net Manager is unable to detect conflicts that allow a service to function normally but may block particular types of traffic, for example, from traveling site to site.

6.3.1 User Group Administration

One of the most common policy errors occurs in the configuration of User Groups for each Corente Services Gateway. User Groups are the groups of machines (such as computers, servers, and printers) on the local network that are allowed to participate in the Corente Services network. Occasionally, a new machine may be added to a customer site LAN and its IP address will not be included in the User Group that is configured to access the application at the hub site.

To view or update the User Groups, do the following:

1. Determine the IP addresses of the machines that cannot access the application.
2. Right-click the Corente Services Gateway icon on the App Net Manager map and select **Edit**. The Location form is displayed.

3. Click the **User Groups** tab of at the top of the Location form.
4. Select **Default User Group** from the list that is displayed and click the **Edit** button at the bottom of the window.
5. In the **User Groups Subnets/Address Ranges** section on this window, are the IP addresses of the machines included in any of the ranges or subnets that are displayed?
6. If not, create a new subnet and address range entry. Select the **Add** button.
   - **Include Subnet:** Select this option to specify a range that will be included in the group. Fill out the available fields as follows:
     - **Network Address:** Enter the first address of the subnet in this field.
     - **Subnet Mask:** Enter the net mask of the subnet in this field, which will define the range of addresses within this subnet.

     Note

     If you include a range of IP addresses that is not contained within the same subnet of the LAN IP Address of the Corente Services Gateway or not distributed by the Corente Services Gateway's DHCP server, you must provide routing information to this subnet on the **Routes** tab or enable **RIPv2** or **OSPF** on the **Network** tab of this form.
   - **Outbound NAT:** You must set the appropriate **Outbound NAT** settings for this subnet. For now, select **Permitted**.
7. Click **OK** to add this definition to this Default User Group.
8. Click **OK** on the on the Default User Group window, and **OK** on the Location form window.
9. Click the **Save** button in the App Net Manager tool bar to save your changes.

Once the changes have been saved and distributed to the Corente Services Gateway, the user should be able to access the application from the new machine.

6.3.2 Routing Configuration Issues for a Peer Corente Services Gateway

Occasionally, routing issues at the hub site or customer site can cause a tunnel to appear green and active in App Net Manager, but actually prevent traffic from correctly traversing the secure tunnel and prevent an application from functioning correctly. This is a common issue for a Corente Services Gateway that is using the Peer configuration.

The **Top Talkers** feature in Gateway Viewer can help verify that traffic is traversing the tunnel, so that you can narrow down the problem to routing issues on the hub site or the customer site.

If the tunnel appears active in App Net Manager and the User Groups are configured correctly, but the customer site is unable to reach hosts on the other side, do the following:

1. Access the customer's Gateway Viewer remotely, from the hub site.

   To do this, ensure that there is a tube configured on both the hub site Corente Services Gateway and the customer site Corente Services Gateway that allows access to the customer's Corente Services Gateway LAN IP address from the hub site.
2. Log in to Gateway Viewer.

3. Click the **Monitoring** button and then click **Top Talkers**. **Top Talkers** displays the top ten most active hosts on the customer's site.
4. Choose one of the hosts listed on this page. Note the IP address of the host, and select the **Set Options** hyperlink.
5. On the **Top Talkers Options** page, in the **Address Ranges** field, enter the IP address of host that you noted in the previous step. Click **Submit** to save your changes. Now on the **Top Talkers page**, data will be displayed for that host only.
6. Open a terminal window and ping the IP address of the host that you chose. If you can see echo requests come through on the **Top Talkers** page, then the issue is most likely due to routing on the customer side, where the return traffic does not have a route that allows traffic back.

Allowing Remote Access to a Corente Services Gateway

To allow remote access to a customer's Gateway Viewer, do the following:

1. In App Net Manager, access the Location form for the Corente Services Gateway by right-clicking on the Corente Services Gateway icon in the map and selecting **Edit**. The Location form is displayed in a new window.
2. On the Location form, click the **Partners** tab. This tab is used to choose the partners of this Corente Services Gateway.
3. The main **Partners** tab presents a table of all partners of the Corente Services Gateway. Select the hub site Corente Services Gateway and click the **Edit** button. The **Edit Partner** screen is displayed.
4. On this screen, click the **Add** button to create a new tube.
5. Select the **Location LAN Address** option from the **Local User Group** pull-down menu.
6. Select a Firewall Policy that allows the **gateway_viewer** Firewall Service both inbound and outbound over the connection, or leave this option set to **None**.
7. Select the **Remote User Group** that contains the IP address of the computer you are currently using, therefore allowing this computer to access the customer's Corente Services Gateway.
8. Click **OK** to store the tube definition. Click **OK** on the **Edit Partner** screen, then **OK** on the Location form, and then click the App Net Manager **Save** button to save your changes.
9. Similar configuration must be performed on the hub site Corente Services Gateway. Access the Location form for the hub site Corente Services Gateway, open the Location form, and access the **Partners** tab.
10. Select the customer's Corente Services Gateway on the **Partners** tab and click the **Edit** button. **Add** a new tube.
11. Select the **Local User Group** that contains the IP address of the computer you are currently using, therefore allowing this computer to access the customer's Corente Services Gateway.
12. Select a Firewall Policy that allows the **gateway_viewer** Firewall Service both inbound and outbound over the connection, or leave this option set to **None**.
13. Click **OK** to store the tube definition. Click **OK** on the **Edit Partner** screen, then **OK** on the Location form, and then click the App Net Manager **Save** button to save your changes.
14. Select the **Location LAN Address** from the **Remote User Group** pull-down menu.

You should now be able to access the customer's Gateway Viewer by typing the LAN IP address of their Corente Services Gateway into a browser.

6.3.3 Recent Administration Changes

You can also check the administrator logs in App Net Manager to see if any recent administrative changes could have caused the issue. To access the administrator logs in App Net Manager, do the following:

1. Double-click the **Reports** category in the domain directory.
2. Double-click the **Logs** subcategory.
3. Double-click the **Administration Logs** subcategory.
4. Select any month to view the logs of administrator activity for that month in a table on the right side of the App Net Manager interface.

A common configuration error to check for in the logs is as follows:

- *Did any administrators recently make changes to any Firewall Policies?*

  Firewall Policies are created once and can then be applied to multiple Corente Services Gateways throughout the Corente Services network to control what type of traffic is allowed over specific partner to partner connections. If any changes are made to an existing Firewall Policy, those changes will be applied automatically to any Corente Services Gateway that is currently using that Firewall Policy. Ensure that any changes made to a Firewall Policy do not block the protocols that your applications require to operate between sites.

  To view the Firewall Policies currently defined in your domain, open the **Global Intranet Settings** category in the domain directory. Open the **Firewall** subcategory and do the following:

  1. Open the **Firewall Policies** subcategory.
  2. Select the **Firewall Policies** subcategory and view the table on the right side of the interface. This table displays the following fields:
     - **Firewall Policy:** The name of the policy.
     - **Out Default:** The default behavior for outbound Firewall Services that are not specified (**Deny**, **Allow**, or **Continue** to the next policy).
     - **Exceptions:** The number of specified Firewall Services for outbound traffic.
     - **In Default:** The default behavior for inbound Firewall Services that are not specified (**Deny**, **Allow**, or **Continue** to the next policy).
     - **Exceptions:** The number of specified Firewall Services for inbound traffic.
     - **Permission:** The Corente Services Gateways that have permission to use this particular Firewall Policy (**All**, **None**, or **Specified**).
     - **In Use:** Whether or not the Firewall Policy is currently in use for any Corente Services Gateway.

  To view the definition of an existing Firewall Policy, open the Firewall Policy's branch in the domain directory. Three categories are displayed: **Inbound**, **Outbound**, and **Policy Use**.

  - Open the **Inbound** or **Outbound** branches to see what Firewall Services have been specified for that direction. A note in brackets for each of these branches will tell you whether the specified Firewall

Services are allowed through the firewall but all other protocols and ports are denied (*Allow Specified/Deny*) or whether the specified Firewall Services are denied through the firewall but all other protocols and ports are allowed (*Deny Specified/Allow*).

- Open the **Policy Use** branch to see which Corente Services Gateways are allowed to use the Firewall Policy in their configurations.

6.4 Troubleshooting Performance Issues

Sometimes there may be issues relating to the performance of the service, rather than a service interruption. If a Corente Services Gateway is functional and active on the Corente Services network, the monitoring tools in Gateway Viewer and App Net Manager enable you to diagnose and resolve performance issues.

6.4.1 Connection Issues to the Hub Site

Performance issues are most often caused by a routing device that is not functioning properly between the customer site and the hub site (also known as a *hop* between sites). Several tests and features in Gateway Viewer and App Net Manager can help determine what hop might be causing latency or loss issues for application traffic. App Net Manager can also help determine whether a gateway is using too much or too little bandwidth.

First, identify whether or not there are any active alerts on the Corente Services Gateway by right-clicking the Corente Services Gateway icon in the App Net Manager and highlighting **Alarms** in the displayed menu. Select an alarm number to view the details of that active alarm. This indicates what sort of problem the Corente Services Gateway is experiencing. When there is a performance issue, this alarm will often indicate whether the issue is due to latency, loss, or bandwidth shortage.

6.4.1.1 Review Latency Data

If there is an issue with slow performance, the issue is most likely a latency problem.

In the Gateway Viewer, on the **Test** page, perform a ping test from the customer's Corente Services Gateway to the hub site. This gives a basic measure of latency. Do the following:

1. In the **Partner** section, click the **Ping** button beside the name of the hub site.
2. The results of this test will display the approximate round trip time of test packets.

If this test indicates that there is latency on the connection to the hub site, the user should next perform a traceroute test to determine what part of the network is experiencing the latency.

1. In the **Partner** section, click the **Traceroute** button beside the name of the hub site.
2. The results of this test display the amount of time it takes for a packet to reach each hop on the way to the hub site.

If the results of the traceroute indicate that the latency is caused at some point on the Internet, contact the ISP to determine the cause of the latency. If the test indicates that the latency is caused by a device at the hub site or on the customer LAN, this issue should be escalated to Oracle Support.

6.4.1.2 Review Packet Loss Data

If a Corente Services Gateway is generating a loss alert, access the **Test** page of Gateway Viewer.

On the **Test** page, perform a ping test from the customer's Corente Services Gateway to the hub site. This gives a basic measure of packet loss.

1. In the **Partner** section, click the **Ping** button beside the name of the hub site.
2. The results of this test display the percentage of loss on packets between the customer site and the hub site. Ideally there should be no loss, and a loss rate exceeding 5% is poor.

If this test indicates that there is an unacceptable amount of packet loss on the connection to the hub site, you should next perform a traceroute test to determine what part of the network is experiencing the latency.

1. In the **Partner** section, click the **Traceroute** button beside the name of the hub site.
2. The results of this test show an asterisk in place of a dropped packet. This can help indicate the point in the route to the hub site at which a packet loss occurs or begins to occur.

If the results of the traceroute indicate that the loss is caused at some point on the Internet, contact the ISP to determine the cause of the loss. If the test indicates that the loss is caused by a device at the hub site or on the customer LAN, this issue should be escalated to Oracle Support.

6.4.1.3 Review Bandwidth Data

If the gateway is generating a bandwidth alert or the previous tests have proved inconclusive, you can examine the bandwidth reports for a Corente Services Gateway in App Net Manager.

To access bandwidth reports in App Net Manager, do the following:

1. Double-click the **Reports** category in the domain directory.
2. In the subcategories that are displayed under **Reports**, double-click the **Graphs** subcategory. All of the Corente Services Gateways in the domain are listed under the **Graphs** subcategory.
3. Double click the Corente Services Gateway name.
4. Select **Bandwidth Report** to view the bandwidth report.

If the report is displaying a consistent excess of bandwidth usage, this could be causing poor application performance. A device on the customer site LAN might be consuming too much bandwidth, causing the application to be slow.

To identify the top bandwidth users on the customer site LAN, access Gateway Viewer and log in and then click the **Monitoring** button and then click **Top Talkers**.

The top ten bandwidth users on the user’s LAN are displayed. You can use this information to identify the cause of the problem.

6.4.2 QoS Settings

An application could be suffering from poor performance due to incorrect QoS (Quality of Service) configuration. If there are multiple applications being used over the Corente Services network, you must make sure that the highest priority applications have the highest QoS priority, and the lowest priority have the lowest.

QoS settings are enabled on the customer side in *tubes*, which divide each site-to-site connection into specific sets of rules that apply to specific User Groups and applications.

1. Access the Location form for the customer's Corente Services Gateway by right-clicking on the Corente Services Gateway icon in the map and selecting **Edit**. The Location form is displayed in a new window.
2. On the Location form, click the **Partners** tab. This tab is used to choose the partners of this Corente Services Gateway.

3. The main **Partners** tab presents a table of all partners of the Corente Services Gateway. Select the hub site gateway and click the **Edit** button. The **Edit Partner** screen will be displayed.
4. On this screen, select a tube that is defined for this connection and click **Edit**. The **Edit Tube** screen is displayed.
5. Ensure that any **Inbound** or **Outbound QoS** settings for this particular User Group to application partnership are the correct priority levels. Change as necessary.
6. Repeat for any additional tubes.
7. When you are finished, click **OK**. Click **OK** again to store your changes to the customer to hub site partnership, and click **OK** once more to store your changes to the Location form.
8. Click the **Save** button on the App Net Manager tool bar to save your changes.
9. Wait a few minutes until the changes have been distributed to the customer's Corente Services Gateway.

   Check that the application performance is improved.

Part I App Net Manager Help

The *App Net Manager Help* is available from the **Help** menu item in App Net Manager. However, because you administer your Corente Services network with App Net Manager, the help content is also included in this part of the *Corente Services Administration Guide*.

Table of Contents

Chapter 7 Overview of App Net Manager

Table of Contents

App Net Manager provides an interface with two main sections:

Domain directory	Displays on the left section of the App Net Manager interface. The domain directory is a navigational structure that contains resources for your Corente Services domain, including your contact information, user settings, intranet settings, and Location configuration.
Domain map and **Detail** tab	Display on the right section of the App Net Manager interface. The map is a graphical representation of your Corente Services domain. The **Detail** tab displays different information when you select items in the domain directory.

7.1 Domain Maps

Maps provide graphical representations of your Corente Services domain. Maps let you monitor status of your Corente Services Gateways to quickly identify and troubleshoot issues.

Maps use icons and line colors to represent various states for Locations and tunnels in your Corente Services network.

Tip

Select **View** and then **Legend** to access descriptions for every icon and state that can display on a map.

7.1.1 Changing Map Backgrounds

You can change the map background to different continents, the world, or custom images. Changes you make to the map background apply to all domain administrators.

Note

When you change the map background, the Location icons stay in the same position. You must manually arrange icons to new geographic coordinates on the map.

To change the map background, right-click on the map and then select **View** and then **Set Background**.

To use a custom image as the map background, you must first specify the location of the image as follows:

1. Right-click the domain name and then select **Preferences**.

   The **Preferences for Domain** ***`domain_name`*** dialog displays.

2. On the **General** tab, specify the appropriate settings in the **Custom Map Image** section and then select **OK**.

Related Information. Using Custom Maps

7.1.2 Arranging Location Icons

You can arrange Location icons as follows:

1. Right-click on the map and then select **View** and then **Arrange Locations**.
2. Select one of the following options:
   - **Manual** lets you move the Location icons to any position on the map.

     To manually arrange Location icons on the map, do the following:

     a. Press and hold the **Ctrl** key.

     b. Select the Location icon you want to move.

        A compass displays on the Location icon.

     c. Drag the Location icon to a new position on the map.
   - **By Zip** automatically arranges Location icons according to ZIP code.

     If a Location does not have a valid ZIP code, it displays at the top right of the map.
   - **Auto** arranges the Location icons at the top of the map.

7.1.3 Loading and Refreshing Alarms

App Net Manager does not automatically load or refresh alarms that occur for Locations.

To load alarms, right-click on the map and then select **Alarms** and then **Load Alarms**.

To refresh alarms, right-click on the map and then select **Alarms** and then **Refresh Alarms**.

The following icon displays on Locations for which alarms exist: ⚠

7.1.4 Changing Map Views

You can change the map view to show only problems in the domain or to focus on

To change the map view, right-click on the map and then select **View** and then one of the following options:

- **All** shows all Locations and tunnels.
- **Problems Only** shows only Locations that are denied or for which an alert exists. This view also shows tunnels that are not current active or for which an alert exists.

- **Active Tunnels** shows only tunnels that have active connections between Locations.
- **Down Tunnels** shows only tunnels that are not currently active.
- **Alert Tunnels** shows only tunnels for which alerts exist.
- **Configuration Alert Tunnels** shows only tunnels for which configuration alerts exist.

7.2 Menus

You can access controls through menus in App Net Manager.

- **File** menu provides the following controls:
  - **Save** displays the **Save All Changes** dialog. You can review all changes and then save them to the Corente SCP. Until you save your changes to the Corente SCP, they are stored locally and do not apply to your domain.
  - **Add** ***`New Item`*** lets you add objects to your domain. For example, when you select the **Locations** folder, this control lets you add a new Location.
  - **Wizards** provides access to dialogs that guide you through common tasks.
    - The **Location** wizard guides you through the steps to create new Locations. You should use the **Location>** wizard after you install and configure a Corente Services Gateway for the first time.
    - The **Download Location** wizard lets you easily download configuration files for Corente Services Gateways.
    - The **Partner Locations** wizard helps you establish partner connections between Corente Services Gateways. Partner connections consist of secure tubes that configure how traffic passes between Corente Services Gateways.
    - The **Tube** wizard helps you configure traffic that passes between Corente Services Gateways.
  - **Exit** closes App Net Manager.
- **Edit** provides controls that let you work with objects in your domain.

  Note

  App Net Manager stores user preferences as cookies. Select **Delete Cookies** to restore the default settings.
- **View** provides the following controls:
  - **Legend** provides descriptions for the icons and states that can display on maps.
  - **Tool Bar** shows and hides the App Net Manager toolbar.
  - **Graphical View** shows the map.
- **Login** lets you log out of App Net Manager and change your password.

  The **Help** menu provides access to documentation and information about App Net Manager. If you need to contact Oracle Support, select **External Ticketing** to open a support request form in your browser.

7.3 Toolbar

The toolbar provides quick access to controls.

Display and hide toolbars as follows:

1. Position your cursor in the space between the menus and the graphical tabs in App Net Manager.
2. Right-click to show the toolbar context menu.
3. Select one of the following options from the toolbar context menu:
   - **File Tool Bar** displays or hides the **New**, **Refresh**, and **Save** options.

     Note

     App Net Manager does not automatically load changes while you are logged in. You must select the **Refresh** button to load changes to items in App Net Manager.

   - **Edit Tool Bar** displays or hides the **Edit**, **Copy**, **Paste**, **Duplicate**, **Delete**, **Find**, and **Show List** and **Show Graphical** options.
   - **Wizard Tool Bar** displays or hides the **Location**, **Download Location**, **Partner Locations**, and **Tube** wizards.
   - **Hide Button Text** hides text labels on buttons in the toolbar.
   - **Show Button Text** displays text labels on buttons in the toolbar.
   - **Hide Tool Bar** hides the toolbar.

     Tip

     If you hide the toolbar, you can display it again from the **View** menu.

7.4 Tab Controls

Right-click a graphical tab in App Net Manager to access the following controls:

Close Tab	Closes the tab in focus.
Close All Tabs	Closes all open tabs.
Disconnect ***`Domain`***	Disconnects from the domain. If you are connected to only one domain, disconnecting logs you out of App Net Manager.

7.5 Drag and Drop

You can drag and drop certain objects in App Net Manager to edit your Corente Services network. Drag and drop provides a simpler, quicker alternative to using copy and paste functions. However, you cannot drag and drop objects from one domain to another. Likewise you cannot drag and drop objects with different permissions.

In general, you can drag and drop objects when performing the following tasks:

- Creating Location partners. If you drag and drop one Location on another Location, the **Location Partnership** wizard launches.

- Adding objects to groups. For example, if you can drag and drop Corente Clients onto Mobile User Groups.
- Copying rules and properties from one object to another. For example, if you drag and drop address ranges from one User Group onto another User Group.
- Copying objects. For example, dragging and dropping a Location onto the Locations item in the domain directory creates a copy of that Location.

Chapter 8 Changing Your Contact Information

You can change your contact and billing information at any time in App Net Manager, as follows:

1. Double-click **Contact Information** in the domain directory.

   The **Edit Contact Information** dialog displays.

2. Change your contact or billing information as appropriate and then select **OK**.

3. Select **File** and then **Save** to save your changes to the Corente SCP.

Chapter 9 Configuring Administrator Accounts

Table of Contents

When you register with Corente Cloud Services Exchange, you specify a name for the root administrator account. As you build your Corente Services network, you can define additional administrator accounts and assign permissions to each account for more granular access to resources.

9.1 Changing the Root Administrator Password

To change the password for the root administrator, do the following:

1. Expand the **Administrators** folder and then right-click the root administrator.
2. Select **Change Password** and specify details on the **Change Password for Administrator** dialog and then select **OK**.
3. Specify details on the **Change Password for Administrator** dialog and then select **OK**.

   A confirmation dialog indicates the password is changed successfully.
4. Select **OK** to close the dialog.

   The password change takes effect immediately but does not require you to log out of App Net Manager.

9.2 Adding Location Groups

You can organize Locations into groups that you can use when assigning administrator permissions, as follows:

1. Expand the **Administrators** folder in the domain directory.
2. Right-click on the **Location Groups** folder and select **Add Location Group**.

   The **Add Location Group** dialog displays.
3. Specify a name for the group then select the Locations you want to add to the group and select **OK**.
4. Select **File** and then **Save** to save your changes to the Corente SCP.

9.3 Adding Local and External Administrators

Local administrators belong to the Corente Services domain to which you are currently connected. External administrators belong to other Corente Services domains.

Tip

Create Location Groups before you add administrators. Location Groups organize Locations to make it easier to assign administrator permissions.

To add administrators, do the following:

1. Expand the **Administrators** folder in the domain directory.
2. Right-click on either the **Local** or **External** folder.
3. Select **Add *X* Administrator**.

   The **Add Administrator** dialog displays.
4. Specify the appropriate settings for the administrator and then select **OK**. See Add Administrator Settings.
5. Select **File** and then **Save** to save your changes to the Corente SCP.

Add Administrator Settings

Settings on the **Add Administrator** dialog are as follows:

Administrator User ID	Specifies a unique ID for the administrator. The ID can be up to 30 alphanumeric characters. The ID can contain underscore characters but not other special characters such as spaces or punctuation. Administrator user IDs must be unique across the Corente Services network, not just a single domain.
Password	Specifies a password that must contain at least one uppercase letter, one lowercase letter, and one number.
Email	Specifies the email address of the administrator.
Phone	Specifies an optional phone number for the administrator.
Pager	Specifies an optional pager number for the administrator.
Challenge Question	Allows administrators to recover lost passwords. If the administrator forgets the password, Oracle Support ask the challenge question to verify the administrator.
Challenge Answer	Provides a response to the challenge question. The value can contain a maximum of 30 alphanumeric characters.
Domain Level Access	Specifies permissions that the administrator has for the domain. You can select the following permissions: • **All Privileges** provides read and write permissions to all objects in the domain. However, only the root administrator can add or edit other administrators. • **Edit Configuration/Location Privileges** provides read permissions to the domain and write permissions all Location configuration settings. • **View Configuration/Location Privileges** provides read permissions to the domain. • **Alarm Viewing Privileges** provides read and write permissions to objects in the **Alarms and Events** folder in the domain directory.

	• **Report Viewing Privileges** provides read and write permissions to objects in the **Reports** folder in the domain directory.
All Location Edit Privileges	Allows administrators to edit existing Locations and create Location partners. This permission does not allow administrators to add or delete Locations.
Specified Location Edit Privileges	Allows administrators to edit and create partners for only the Locations that you specify.

Chapter 10 Configuring Global Intranet Settings

Table of Contents

The **Global Intranet Settings** category in the domain directory contains features that apply to all of the Locations within a domain.

10.1 Firewalls

Firewalls prevent unwanted traffic from compromising your company's security. The firewalls that are available on a Corente Services Gateway allow you to control both the inbound and outbound traffic that is allowed over multiple types of connections, from other locations in the application network, the Internet, or the LAN, to and from your Corente Services Gateway and the LAN.

You should begin the process of connecting your Locations by defining the firewalls that you will use to protect your corporate networks. To begin managing firewalls with App Net Manager, you define Section 10.1.1, “Firewall Services”. These are the protocols (such as UDP, TCP, or ICMP) and Source/Destination Port Numbers (or ICMP type) used by certain programs and services. Next, you define Section 10.1.2, “Firewall Policies” by assembling groups of Firewall Services to either allow or deny over inbound and outbound connections. Firewall Policies are then administered on the LAN-to-partner, LAN-to-Internet, and LAN-to-Location connections.

To access the Firewall features, open the **Global Intranet Settings** category in the domain directory of App Net Manager. Open the **Firewalls** subcategory, and both the Firewall Services and Firewall Policies features will be displayed. Any definitions that you change or create will be stored for use by all administrators of your domain.

10.1.1 Firewall Services

Firewall Services are combinations of protocols (UDP, TCP, or ICMP) and Source / Destination Port Numbers (or ICMP type) that are used by certain programs and services.

Corente Cloud Services Exchange automatically provides the following predefined Firewall Services:

- domain (for access to App Net Manager)
- ftp (for file transferring)
- gateway_viewer (for access to Gateway Viewer)
- http (for web browsing)

- https (for SSL-encrypted web browsing)
- icmp (to test for connectivity and search for configuration errors in a network.)
- imap (for e-mail) netbios (for file-sharing)
- ntp (to synchronize the time on a computer to a server or reference time source over the application network)
- pop3 (for e-mail)
- smtp (for e-mail)
- smnp (for monitoring Corente Services Gateways or network devices with SNMP)
- ssh (for secure telnet)
- telnet (to log into computers with telnet)
- tftp (for improved FTP file transferring)
- ldap (for authentication)
- radius (for authentication)
- syslog (for logging)

To view the Firewall Services that are currently defined in your domain, do the following:

- Open the Firewall Services branch in the domain directory.
- Click Firewall Services in the domain directory and view the table on the right side of the interface. This table lists the following:
  - **Firewall Service:** The name of each service
  - **Default:** Whether or not the service is a Default service
  - **Rules:** How many rules the service contains

To view the rules of an existing Firewall Service, open the Firewall Service in the domain directory or select the Firewall Service name in the table on the right side of the interface.

You can use the **Edit** or **Delete** buttons in the toolbar of App Net Manager to edit or delete an existing Firewall Service. You cannot edit or delete a default Firewall Service. Changes made to a Firewall Service will change the personality configuration of any Locations using that particular service.

If you delete a Firewall Service currently in use by any of your Locations, the Locations will no longer be able to use this service and the service will be deleted from the definitions of any existing Firewall Policies.

Add a New Firewall Service

If you are planning to share applications that require Firewall Services that differ from the default Firewall Services, you can define the rules of additional Firewall Services.

Note

Because Corente Cloud Services Exchange firewalls are stateful, you do not need to define Firewall Services for return traffic of any of the common protocols.

To create a new Firewall Service, make sure Firewall Services is selected in the domain directory and do the following:

- Select the **New** button in the toolbar.
- From the **File** menu, select **Add Firewall Service**.
- Right-click **Firewall Services** in the domain directory and select **Add Firewall Service**.

A blank Add Firewall Service window is shown.

Complete the fields in this window as follows:

- **Firewall Service Name:** Enter a name for your new Firewall Service. This name may contain up to 30 alphanumeric characters. Underscores are allowed, but do not use tabs, spaces, or punctuation marks when creating this name.
- **Firewall Service Rules:** App Net Manager defines each set of protocols and port ranges in a Firewall Service as a rule. A single Firewall Service can contain multiple rules. This will occur if the program for which you are creating a Firewall Service operates over several different ranges of port numbers or uses several types of protocols. Each Firewall Service you create can be used in one or more Firewall Policies.

  The Firewall Service Rules table displays each rule by protocol type and either source and destination range or ICMP type. To edit an existing rule, select the rule and click the **Edit** button.

  To delete an existing rule, select the rule and click the **Delete** button.

  To add rules to your Firewall Service, click the Add button at the bottom of the window. The **Add Firewall Service Rule** window will be displayed.

On this window, complete each of the following fields:

- **Protocol:** Choose the type of protocol from the following list of options: TCP, UDP, and ICMP. This designates the type of packet that will be entering and exiting the ports. The protocol you choose in this menu will determine what other options on this screen are enabled.

  When TCP or UDP is selected, the following options are enabled:

  - **Source Port Range** specifies ports in the range from 1 to 65534. Select **Any** to allow all ports.
  - **Destination Port Range** specifies a range of up to 15 ports.
- When ICMP is selected, the adjoining menu is enabled:
  - **ICMP Type:** Select the type of ICMP from this pull down menu. You can choose from Any, 0 (Echo Reply), 3 (Dest Unreachable), 4 (SRC Quench), 5 (Redirect), 8 (Echo Request), 9 (Router Adv), 10 (Router Sol), 11 (Time Exceeded), 12 (Param Problem), 13 (Timestamp Req), 14 (Timestamp Rep), 15 (Info Req), 16 (Info Rep), 17 (Addr Mask Req), and 18 (Addr Mask Rep).

  After you have completed these fields, click **OK** to add this rule to your Firewall Service or **Cancel** to close the window without saving your selections. You can add as many rules to a Firewall Service as you would like using this procedure.

When you have completed the entire definition of your new Firewall Service, click **OK** to store your changes or **Cancel** to close the window without storing. Your new Firewall Service will now appear in the domain directory and on the table on the right side of the screen.

Note that you must save your changes in order for your additions to take effect.

10.1.2 Firewall Policies

Firewall Policies are groups of Firewall Services. Each policy constitutes a firewall definition that, when enabled on a connection, can provide customized access control between a Corente Services Gateway and its LAN, its partners, and the Internet. Each Corente Services Gateway User Group and tube associated with a particular Location can be assigned a unique Firewall Policy, to prevent specific users, on either end of the connection, from using certain applications and protocols across the connection.

To view the Firewall Policies currently defined in your domain, do the following:

- Open the Firewall Policies branch in the domain directory.
- Select Firewall Policies in the domain directory and view the table on the right side of the interface. This table displays the following:
  - **Firewall Policy:** The name of the policy.
  - **Out Default:** The default behavior for outbound Firewall Services that are not specified (Deny, Allow, or Continue to the next policy).
  - **Exceptions:** The number of specified Firewall Services for outbound traffic.
  - **In Default:** The default behavior for inbound Firewall Services that are not specified (Deny, Allow, or Continue to the next policy).
  - **Exceptions:** The number of specified Firewall Services for inbound traffic.
  - **Permission:** The Locations that have permission to use this particular Firewall Policy (All, None, or Specified).
  - **In Use:** Whether or not the Firewall Policy is currently in use for any Location.

To view the definition of an existing Firewall Policy, open the Firewall Policy's branch in the domain directory. Three categories are displayed: Inbound, Outbound, and Policy Use.

- Open the Inbound or Outbound branches to see what Firewall Services have been specified for that direction. A note in parenthesis for each of these branches will tell you whether the specified Firewall Services are allowed through the firewall but all other protocols/ports are denied (Allow Specified/Deny) or whether the specified Firewall Services are denied through the firewall but all other protocols/ports are allowed (Deny Specified/Allow).
- Open the Policy Use branch to see what Locations are allowed to use the Firewall Policy in their personalities.

Selecting a Firewall Policy will display a graphical representation of the Firewall Policy on the right side of the interface that enables you to quickly view or edit that policy.

You can also use the **Edit** or **Delete** buttons in the App Net Manager toolbar to modify any existing Firewall Policy. Changes made to a Firewall Policy will change the personality configuration of any Locations using that particular service. If you delete a Firewall Policy currently in use by any of your Locations, the Locations will no longer be able to use this policy and will revert to the default policy for the corresponding type of connection.

Default Firewall Policies

Several predefined Default Policies are available in App Net Manager. The names of each of these Default Policies describe a connection that is possible to configure between Locations or Locations and Remote

Users. These policies have been preconfigured, but can be modified and apply by default to all of the connections in your domain that correspond with their name. App Net Manager also enables you to define additional policies that can be used instead, such as those to be used for specific Locations.

When you create a tube, by default, the applicable Firewall Policy will be enabled on that tube. You can replace this Default Firewall Policy with another Default or Custom Policy, if you want to.

- **DMZ to Internet:** This Firewall Policy is the default for how the Internet and your DMZ (if applicable) are allowed to contact each other via the Corente Services Gateway.
- **LAN to Client:** This Firewall Policy is the default for all remote users-to-Location tunnels and describes how remote users are allowed to access the Location's LAN.
- **LAN to DMZ:** This Firewall Policy is the default for how the LAN and your DMZ (if applicable) are allowed to contact each other via the Corente Services Gateway.
- **LAN to Extranet LAN:** This Firewall Policy is the default for all Location-to-Location tunnels between a Location in your domain and a Location within the domain of an Extranet partner.
- **LAN to Internet:** This Firewall Policy is the default for how each LAN is allowed to contact the Internet through its local Location gateway.
- **LAN to Location:** This Firewall Policy is the default for how each LAN is allowed to contact its local Corente Services Gateway.
- **LAN to Remote LAN:** This Firewall Policy is the default for all Location-to-Location tunnels inside your domain.

Add a New Firewall Policy

To define a Firewall Policy, do the following:

- If defining an existing Default Policy, select that policy and click the **Edit** button in the App Net Manager toolbar.
- If defining a new Custom Policy, make sure Firewall Policies is selected in the domain directory and do the following:
  - Select the **New** button in the toolbar.
  - From the **File** menu, select **Add Firewall Policy**.
  - Right-click **Firewall Policies** in the domain directory and select **Add Firewall Policy.**

The Add Firewall Policy window is displayed.

Note

Because these firewalls are stateful and a pseudo connection state is created for connectionless protocols like ICMP, you need only configure a Firewall Policy for connection initiation and not for return traffic. In addition, this service includes a fixup module for active FTP so that Firewall Policies will automatically permit the appropriate return connection for FTP.

Complete each of the following fields and options:

- **Firewall Policy Name:** If this is not a Default Firewall Policy, enter a name for your new Firewall Policy. This name may contain up to 30 alphanumeric characters. Underscores are allowed, but do not use tabs, spaces, or punctuation marks when creating this name.

- **Outbound Firewall Policy:** The settings in this section affect all outbound connections in the tube on which this Firewall Policy is applied.
  - **Allow/Deny Selected Firewall Services:** Before selecting Firewall Services for the outbound definition of this policy, choose either **Deny** or **Allow** from the pull-down menu. Note that it is generally more secure to select the Allow option and ban all services but the few that you specify, rather than to select the Deny option and allow all services over the connection besides the few that you specify.
    - When Deny is selected, choose Firewall Services from the Selected Firewall Services list to indicate the traffic that you would like to restrict from passing outbound through the firewall. All other outbound traffic will not be denied by this policy. You must then choose how to handle this non-denied traffic, using the Allow/Continue if no match on selected Services option.
      - When Allow is selected and this Firewall Policy is applied to a tube, if the traffic is not explicitly denied, the outbound traffic will be allowed to continue to its destination through this tube.
      - When Continue is selected and this Firewall Policy is applied to a tube, if the traffic is not denied by the tube definition, the traffic will be forced to continue and try the next tube to see if it is allowed or denied by that definition. This option should not be selected in the Firewall Policy of the last tube in a partner connection, to ensure that the traffic that you do not want to block will reach its appropriate destination.
    - When Allow is selected, choose Firewall Services from the list to allow outbound through the firewall. You must then choose how to handle traffic that is not allowed by the firewall, using the Deny/Continue if no match on selected Services option.
      - When Deny is selected and this Firewall Policy is applied to a tube, if the traffic is not explicitly allowed in the tube definition, the outbound traffic will be blocked by the tube or rerouted to the Internet, if backhaul is enabled.
      - When Continue is selected and this Firewall Policy is applied to a tube, if the traffic is not explicitly allowed outbound by the tube definition, the traffic is allowed to continue and try the next tube to see if it is allowed or denied by that definition. This option should not be selected in the Firewall Policy of the last tube in a partner connection, to ensure that the appropriate traffic is blocked from reaching its destination and breaching the security of the firewall.
- **Selected Firewall Services:** All Firewall Services, including both default services and custom services, that are defined in your domain's Firewall Services list will be available for selection in this list.
- **Inbound Firewall Policy:** The settings in this section affect all inbound connections in the tube on which this Firewall Policy is applied.
  - **Deny/Allow Selected Services:** Before selecting Firewall Services for the inbound definition of this policy, choose either **Deny** or **Allow** from the pulldown menu. Note that it is generally more secure to select the Allow option and ban all services but the few that you specify, rather than to select the Deny option and allow all services over the connection besides the few that you specify.
    - When Deny is selected, choose Firewall Services from the list to indicate the traffic that you would like to restrict from entering inbound through the firewall. All other inbound traffic will not be denied by the firewall. You must then choose how to handle this non-denied traffic, using the Allow/Continue if no match on selected Services option.
      - When Allow is selected and this Firewall Policy is applied to a tube, if the traffic is not explicitly denied, the inbound traffic will be allowed to continue to its destination through this tube.

    - When Continue is selected and this Firewall Policy is applied to a tube, if the traffic is not denied by the tube definition, the traffic will be forced to continue and try the next tube to see if it is allowed or denied by that definition. This option should not be selected in the Firewall Policy of the last tube in a partner connection, to ensure that the traffic that you do not want to block will reach its appropriate destination.

  - When Allow is selected, choose Firewall Services from the list to allow inbound through the firewall. You must then choose how to handle traffic that is not allowed by the firewall, using the Deny/Continue if no match on selected Services option.

    - When Deny is selected and this Firewall Policy is applied to a tube, if the traffic is not explicitly allowed by the tube definition, the inbound traffic will be blocked by the tube, or rerouted to the Internet, if backhaul is enabled.

    - When Continue is selected and this Firewall Policy is applied to a tube, if the traffic is not explicitly allowed inbound by the tube definition, the traffic is allowed to continue and try the next tube to see if it is allowed or denied by that definition. This option should not be selected in the Firewall Policy of the last tube in a partner connection, to ensure that the appropriate traffic is blocked from reaching its destination and breaching the security of the firewall.

- **Selected Firewall Services:** All Firewall Services, including both default services and custom services, that are defined in your domain's Firewall Services list will be available for selection in this list.

Firewall Policy Use

When you create a Custom Firewall Policy, you can specify which Locations in your application network will be allowed to enable this policy on their User Groups or tubes. Default Policies are available for use by all Locations.

To configure the use of a Custom Policy, click the **Configure** button. The Edit Firewall Policy Use Permissions window will be displayed.

Complete this screen as follows:

- **Allow all Locations to use Firewall Policy:** Select this option to make this Firewall Policy available to all Locations in your domain.

- **Allow only Selected Locations to use Firewall Policy:** To restrict the Locations in your domain that can enable this Firewall Policy on their connections, select this option. The names of all Locations within the domain will be displayed in the **Selected Locations** list. To allow a Location to use the Firewall Policy, select the checkbox next to the Location's name. Select as many Locations that should use this policy.

Click the **OK** button to store your changes or the **Cancel** button to close the window and discard your changes.

When you have completed configuration of this new Firewall Policy, click the **OK** button to store your changes or **Cancel** to close the window and discard your changes.

You must save your changes in order for your addition to take effect.

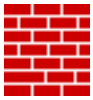
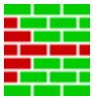
Firewall Policy Interface

When you select a Firewall Policy in the domain tree or the Firewall Policy table, a graphical representation of the Firewall Policy will be displayed on the right side of the interface.

All of the Firewall Services that have been defined in your domain will be listed in a column in the middle of the screen. On either side of this column are brick walls, representing the firewall both outbound and inbound.

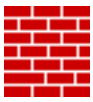
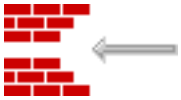
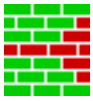
The first wall, on the left, represents the outbound side of the firewall. The following table describes the icons on the outbound side.

Table 10.1 Guide to Outbound Firewall Icons

Icon	Meaning
	By default, all unspecified Firewall Services are denied outbound, and this particular Firewall Service is denied outbound.
	By default, all unspecified Firewall Services are denied outbound, but this particular Firewall Service is allowed outbound.
	By default, all unspecified Firewall Services are allowed outbound, and this particular Firewall Service is allowed outbound.
	By default, all unspecified Firewall Services are allowed outbound, but this particular Firewall Service is denied outbound.

The second wall, on the right, represents the inbound side of the firewall. The following table describes the icons on the inbound side.

Table 10.2 Guide to Inbound Firewall Icons

Icon	Meaning
	By default, all unspecified Firewall Services are denied inbound, and this particular Firewall Service is denied inbound.
	By default, all unspecified Firewall Services are denied inbound, but this particular Firewall Service is allowed inbound.
	By default, all unspecified Firewall Services are allowed inbound, and this particular Firewall Service is allowed inbound.
	By default, all unspecified Firewall Services are allowed inbound, but this particular Firewall Service is denied inbound.

You can quickly modify a Firewall Policy on this interface by right-clicking on either the outbound or the inbound walls beside a Firewall Service.

- To allow a particular Firewall Service outbound (or inbound) when the firewall is denying that Firewall Service, place your cursor over the section of the wall representing the outbound (or inbound) side of the firewall beside that service.

Your cursor will change to , which indicates that you can choose to allow this service. Right-click your mouse button and select Allow Outbound (or Inbound) Traffic. A dialog box will appear to confirm your action. Select **OK**.

- To deny a particular Firewall Service outbound (or inbound) when the firewall is allowing that Firewall Service, place your cursor over the section of the wall representing the outbound (or inbound) side of the firewall beside that service.

  Your cursor will change to , which indicates that you can choose to deny this service. Right-click your mouse button and select Deny Outbound (or Inbound) Traffic. A dialog box will appear to confirm your action. Select **OK**.

After making your changes, remember to save them.

10.2 SNMP

The Simple Network Management Protocol (SNMP) is a protocol used to monitor network performance and certain aspects of network devices.

To monitor Corente Services Gateways with SNMP, you complete the SNMP tab and the Alerts tab in the Location form. You must also use two tools that are available in the SNMP category of the App Net Manager domain directory:

- Section 10.2.2, “SNMP Views”
- Section 10.2.1, “SNMP Users”

To determine how you will configure SNMP for use with your Corente Services network, review the following summary of the procedure you will need to complete:

1. Identify the SNMP MIBs and MIB objects that provide the information you need to monitor.

   You can view the MIBs that are available for use with a Corente Services Gateway by accessing Gateway Viewer and opening the Download page. Each MIB is listed on this screen with a corresponding text file that you can download. This text file contains the definitions of all objects (for example, SNMP variables) within that MIB.

2. After identifying the MIBs and MIB objects that provide the information you need, you must then create logical groups of these MIBs and MIB objects on the Section 10.2.2, “SNMP Views” interface.

3. Identify the Corente Services Gateways you will be monitoring (if using SNMP v1 or v2) or the users who will be monitoring the Corente Services network (if using SNMP v3).

   - If using SNMP v1 or v2, assemble these Locations into logical groups and give each group a name. Administer an **SNMP Community** for each group. This requires configuration on the machine that will be performing the polls/receiving the traps.

   - If using SNMP v3, administer user accounts on the Section 10.2.1, “SNMP Users” interface.

4. Identify the IP addresses of the machines that will be performing the SNMP queries/receiving the SNMP traps (the **SNMP Managers**). Create User Groups on the User Group tab of the Location form for these machines. For SNMP Managers that are receiving traps, they must each be placed in their own User Group.

5. You **must** make sure that the User Groups containing the SNMP Managers can access this Corente Services Gateway. This may require the configuration of special **tubes** to this Location.

   - To allow **local** computers on the Corente Services Gateway's LAN the ability to monitor this Corente Services Gateway, modify the **LAN to Location** tube on the Partners tab of the Location form or with the **Tubes Wizard**.

   - To allow **remote** computers behind a Location partner the ability to monitor this Location gateway, you can create a specific tube from a remote User Group to the local **Location LAN Address**.

   Any Firewall Policy that is configured between an SNMP Manager's User Group and this Corente Services Gateway must allow the **SNMP** Firewall Service over the connection.

6. Combine the information compiled in the previous steps and decide which views must be used to access which **SNMP Communities** (if using SNMP v1 or v2) and which **SNMP Users** require the use of which views (if using SNMP v3). Also, decide which **SNMP Managers** and their respective User Groups need access to which communities (v1/v2) or which users will be using each SNMP Manager and its respective User Group (v3).

   Complete the configuration of SNMP by providing this information on each SNMP tab of the Location form for each Corente Services Gateway that will be monitored.

7. Finally, if you are using SNMP traps, you must enable the alerts you would like traps sent for on the Alerts tab of the Location form for each Location.

10.2.1 SNMP Users

SNMP v3 requires the use of user accounts to query entities. The **SNMP Users** feature enables you to add user accounts to your Corente Services network that can be used to obtain information from a Corente Services Gateway.

To access the SNMP Users feature, open the **Global Intranet Settings** category of the domain directory, then open the **SNMP** subcategory, and then select **SNMP Users**.

When you select SNMP Users, all SNMP User accounts that have been configured in this domain will be displayed in a table to the right of the domain directory. This table displays:

- **SNMP User:** the SNMP User account name
- **Authorization Type:** the Authorization Type that the account uses
- **SNMP Views:** the number of SNMP Views that have been assigned to them
- **In Use by Traps:** whether or not the SNMP User account is currently in use by a Location

You can edit or delete any existing user. To add a new user, make sure **SNMP Users** is selected in the domain directory and:

1. Select the **New** button in the toolbar.
2. From the **File** menu, select **Add SNMP User**.
3. Right-click **SNMP Users** in the domain directory and select **Add SNMP User**.

   You will be taken to a blank **Add SNMP User** window.

4. Fill out this window as follows:

- **SNMP User Name:** Enter the username for this user. You may use up to 30 alphanumeric characters. Hyphens and underscores are allowed, but do not use tabs, spaces, or punctuation marks when creating this name.
- **Authorization Type:** Choose the type of authentication for SNMP users that is being used on your LAN. You can choose either MD5 or SHA.
- **Authorization Pass Phrase:** Enter the pass phrase for this user.
- **Confirm Pass Phrase:** Re-enter the pass phrase to confirm it and avoid mistakes.
- **Selected SNMP Views:** All views that you have created with the SNMP Views feature will be listed. Select the checkbox beside the view that you would like to assign to this user. Select as many views as you would like to assign. **Select All** will select all views in this list while **Clear All** will clear all of your current choices.

5. When you click the **OK** button and then save your changes with the **Save** button in the App Net Manager toolbar, the new user will be added to the **SNMP Users** list in the domain directory.

10.2.2 SNMP Views

The SNMP Views feature enables you to define groups of MIBs and MIB objects that can later be allowed or denied on each Corente Services Gateway (on the SNMP tab of the Location form) or SNMP User, to limit how SNMP Managers can query or monitor the Corente Services Gateway.

To access the SNMP Views feature, open the **Global Intranet Settings** category of the domain directory, then open the SNMP subcategory, and then select **SNMP Views**.

When you select **SNMP Views**, all SNMP Views that have been configured in this domain will be displayed in a table to the right of the domain directory. This table displays:

- **SNMP View:** the SNMP View name
- **SNMP MIB Subtrees:** the SNMP MIB subtrees that are included in the view
- **In Use Locations:** whether or not the SNMP View is currently in use by a Location
- **In Use SNMP Users:** whether or not the SNMP View account is currently assigned to a SNMP User account

You can edit or delete any existing SNMP View. To add a new SNMP View, make sure **SNMP Views** is selected in the domain directory and:

1. Select the **New** button in the toolbar.
2. From the **File** menu, select **Add SNMP View**.
3. Right-click **SNMP Views** in the domain directory and select **Add SNMP View**.

   You will be taken to a blank **Add SNMP View** window.

4. **SNMP View Name:** Enter a name for your new view in this field. You may use up to 30 alphanumeric characters. Hyphens and underscores are allowed, but do not use tabs, spaces, or punctuation marks when creating this name.

SNMP MIB Subtrees

You can Edit or Delete any existing entries in the table. To add a new entry, click the **Add** button to display the **Add SNMP MIB Subtree** window.

Fill out the following fields:

- **Include SNMP MIB Subtree/Exclude SNMP MIB Subtree:** Select one of these options to include or exclude a MIB (or MIB object) in this view.
- **SNMP MIB Subtree:** Type the name of the MIB (and MIB object, if applicable) in this field that you are including or excluding in the view. If you are specifying a MIB object, use this format: `MIB name::MIB object name`.

When you have completed these fields, click the **OK** button to store your changes or the **Cancel** button to close the window without storing your changes.

Each SNMP View can contain multiple entries. When you have completed the definition of your new view, click the **OK** button to store your changes or the **Cancel** button to close the window without storing your changes. You must save your changes with the **Save** button in the App Net Manager toolbar in order for them to take effect.

10.3 Quality of Service (QoS)

The QoS feature enables you to define different levels of priority that can be set on Corente Services network traffic according to application, User Group, or specific Location-to-Location connection. This traffic is marked so that Corente Services Gateway Locations will obey the prioritization as well as any other device that follows a similar marking scheme. Corente Cloud Services Exchange utilizes both Differentiated Services Code Point (DSCP) and internal priority queuing to ensure traffic prioritization.

By default, App Net Manager provides a set of predefined QoS Entries. These are standard QoS classifications, but you can create custom QoS entries as well.

To view the QoS Entries currently defined in your domain, do the following:

- Open the **Quality of Service** branch in the domain directory.
- Click **Quality of Service** in the domain directory and view the table on the right side of the interface. This table displays the following:
  - **QoS Entry:** The name of the QoS Entry.
  - **DSCP Value:** The DSCP Value for the QoS entry.
  - **Priority:** The priority level for the QoS entry.
  - **Permission:** The Locations where the QoS entry can be used.
  - **Default:** Whether or not the QoS entry is a default service.

Important

When performing any sort of QoS configuration, administrators must be careful when assigning QoS levels because if there is too much high priority traffic, any other traffic with a lower level of priority may become too slow or even be dropped.

You edit or delete an existing QoS Entry with the **Edit** and **Delete** buttons in the App Net Manager toolbar. You will be unable to delete a **Default QoS Entry**. While you cannot modify the definition of a Default QoS

Entry, you can modify the Locations Using this Entry option. Changes made to a QoS Entry will change the personality configuration of any Locations using that particular QoS Entry. If you delete a QoS Entry currently in use by any of your Locations, the Locations will stop using the entry and must be assigned a new entry if you would like them to continue using QoS.

Add a New QoS entry

To define a Custom QoS entry, make sure **Quality of Service** is selected in the domain directory and do the following:

- Select the **New** button in the toolbar.
- From the **File** menu, select **Add QoS Entry**.
- Right-click **Quality of Service** in the domain directory and select **Add QoS Entry**.

A blank **Add QoS Entry** window is displayed.

Complete the fields in this window as follows:

- **Name:** Enter the name that this QoS entry will be called on screens in App Net Manager.
- **DSCP Value:** Select the value that identifies how traffic associated with this QoS entry will be labeled for prioritization on devices within your network. Possible values are between 1 and 63. For example, on your network, all IP telephony traffic may be labeled as a "5" and your routers are configured to recognize this label and prioritize traffic accordingly.
- **Priority:** Select the priority level that explains how the traffic associated with this DSCP entry will be prioritized between Locations (low, medium, or high). This enables you to assign certain traffic a DSCP Value of 5, for example, then further define that traffic by defining three separate QoS entries with a DSCP Value of 5 and a Priority level of either High, Medium, or Low. All High level traffic, no matter what DSCP level, will have the highest priority when sent between Locations, but may be prioritized differently within your network according to its DSCP Value.
- **Locations using this QoS Entry:** Select one of the following choices in this section:
  - **Allow All Locations to use QoS Entry:** Select this option to allow this QoS entry to be enabled on traffic originating or terminating on any Location.
  - **Allow only Selected Locations to use QoS Entry:** Select this option if you would like to limit the use of this QoS entry to only specific Locations within your domain. This is the default. When this option is selected, you must choose the Locations in your domain that can enable this QoS entry on any of their defined applications, User Groups, or tubes, or else this entry is not available for use by any Locations. To choose Locations, select the checkbox beside each Location name in the Selected Locations list. The Select All button will select all the boxes in the list, and the Clear All button will clear your selections. You may permit as many Locations as you would like to use the QoS Entry.

When you are finished defining the QoS Entry, select the **OK** button to store your changes or the **Cancel** button to close the window without storing. Note that you must **Save** in order for any additions to take effect.

Enable QoS on an Application, User Group, or Tube

After you have assigned the use of QoS entries to Locations within your Corente Services network, you can enable these entries on the applications, User Groups, and tubes that you choose, on the Corente Services Gateways that you have allowed these entries to be used on. Corente Cloud Services Exchange

allows separate prioritization choices for both inbound and outbound traffic. You cannot use QoS to prioritize traffic to or from a Corente Client.

Traffic that has been placed in similar priority queues (high, medium, or low) will be routed with the same prioritization within the Corente Services network.

10.4 User Remote Access

You provide remote and traveling users with Mobile User accounts in App Net Manager so that they can connect to Corente Services Gateways and access resources at your main office locations.

Mobile Users can remotely access a Corente Services network using:

- **Mobile Devices:** You configure secure mobile user access for iOS and Android devices in App Net Manager.
- **Oracle Corente Client:** Users with Microsoft Windows devices install a Corente Client that uses Internet Protocol Security (IPsec) for secure access.

You can find more information about setting up Mobile Users in the *Corente Services Administration Guide*.

Note

In previous releases, the **Client Administration** feature of App Net Manager was used to configure Corente Client accounts. The Client Administration feature is now reserved for managing legacy Corente Clients.

10.4.1 Mobile Users

You configure Mobile Users in App Net Manager to provide remote access to you Corente Services network.

10.4.1.1 Viewing Mobile Users

To view Mobile Users that are configured in App Net Manager, do the following:

1. If necessary, manually refresh the Mobile User data in App Net Manager.
   a. Expand the **Global Intranet Settings** menu in the domain directory.
   b. Expand **User Remote Access** and then select and right-click **Mobile User Administration**.
   c. Select **Refresh/Clear Changes**.
2. Expand the **Global Intranet Settings** menu in the domain directory.
3. Expand **User Remote Access** and then expand **Mobile User Administration**.
4. Select **Mobile Users**.

The following fields display for each Mobile User:

Mobile User	Displays the Mobile User account name.
Number of Group Memberships	Displays how many Mobile User Groups the Mobile User belongs to.

External Authentication	Indicates if the Mobile User authenticates with the Corente Services Gateway using an external authentication provider.
Helper App	Indicates if the Mobile User connects to the Corente Services Gateway with the Corente Client.
Expires	Displays the number of days until the Mobile User account expires, if applicable.
Connected to Location	Indicates if the Mobile User is currently connected to a Corente Services Gateway and displays that Corente Services Gateway name.
Last Contact	Indicates the last time the Mobile User connected to the Corente SCP. Applies to Mobile Users who connect with the Corente Client.

The following icons also display status for Mobile Users:

Icon	Status	Meaning
	Up	The Mobile User is currently connected.
	Down	The Mobile User is not currently connected.
	Expired	The Mobile User account is no longer active.

10.4.1.2 Adding Mobile Users

To add a new Mobile User, select **Mobile Users** and click the **New** button.

The Add Mobile User window is displayed. On this window, fill out the fields as follows:

- **Name:** Enter a name for the new Mobile User.

  You can use up to 50 alphanumeric characters, including hyphens and underscore characters. Tabs, spaces, and punctuation characters are not allowed.

  Mobile User names cannot be the same as any Location names or existing Corente Client account names in your domain.

  If you plan to configure an external authentication provider, the Mobile User name must match the login name in the directory.

- **Email:** Email address of the Mobile User

  A confirmation email message is sent to the user when you set up a Mobile User account.

- **Use External Authentication:** Select this option and the Mobile User will authenticate using either RADIUS or LDAP, depending on the type of external authentication that has been enabled on the Corente Services Gateway. See Section 11.9.9.3, “Configuring External Authentication”.

  Note

  If an External Authentication server has not been enabled on the Corente Services Gateway, the Mobile User will be unable to connect to the Location.

- **Password:** Create an alphanumeric password for this Mobile User account. This password must contain at least one uppercase, one lowercase, and one numeric character.

- **Confirm Password:** Re-enter the password you created in the **Password** field to avoid any mistakes.
- **Windows Helper App Settings:** These settings only apply if the Mobile User is using the Corente Client on a Windows client device.

  Select the **Use in Conjunction with Windows Helper App** check box and configure the following settings:

  - **Access Settings:** Allows you to select how the Corente Client will connect to your Corente Services network.
    - **Allow access to local Network:** Select this option if you would like to allow the Corente Client to contact and be contacted by machines on its own LAN while it is connected to its Location partner. You should not select this option if this machine will be accessible by untrusted devices. When this option is **not** selected, while the software is in use, the Corente Client will only be able to contact and be contacted by machines via the Location partner. By default, this option is not selected.
    - **Backhaul All Traffic:** Select this option if you would like all traffic (both traffic destined for the Location partner and traffic destined for other places, such as the Internet) to travel inside the secure tunnel and be routed to the Location partner. The Location partner receives all of the traffic and then routes it appropriately. By default, this option is selected. When this option is **not** selected, no traffic will be backhauled. This means that the Corente Client:
      - Is able to access only the computers on the LAN of the Location to which it is connected.
      - Is unable to access the partners of its Location partner. The partners and computers behind those partners will be visible to the Corente Client user in Gateway Viewer, but will be inaccessible.
  - **Mobile User Expiration:** If you would like to create a temporary Mobile User account for a user, you can use the **Mobile User Expiration** feature to specify the length of time (in days) that the user will be permitted to connect to its partners. When the subscription period has ended, the Mobile User will immediately be disconnected by the Corente SCP when the user attempts to connect to partners. An expired Mobile User account will remain listed in App Net Manager so that you are able to modify the **Mobile User Expiration** settings and renew the Mobile User subscription, easily rendering the Mobile User account usable again.
    - **No Expiration:** When this option is selected, the subscription for this Mobile User will not expire. The Mobile User will be permitted to connect to its partners until you delete this Mobile User account or change the **Mobile User Expiration** settings. By default, this option will be selected.
    - **Expires In:** When this option is selected, the Mobile User subscription will endure for the time period that is specified in the adjacent field. When the end of the time period approaches, the Mobile User will be notified of the impending expiration. When the time period has ended, this Mobile User will no longer be permitted to connect to its assigned partners until you change the **Mobile User Expiration** settings. The default time period is 30 days.
    - **Expired:** When this option is selected, the subscription for this Mobile User has expired. The Mobile User will not be permitted to connect to its assigned partners unless you renew the subscription by selecting either the **No Expiration** or **Expires In** option and save your changes.
- **Mobile User Group Assignments:** Select the Mobile User Groups to which this new Mobile User will be assigned. You can select as many groups as you would like. A Mobile User Group may contain up to 100 Mobile Users.

When you have finished filling out this window, click **OK** to save your changes. Click **Cancel** to cancel adding the new Mobile User.

10.4.2 Mobile User Groups

Mobile Users are combined into groups to make partner administration easier.

10.4.2.1 Viewing Mobile User Groups

To view Mobile User Groups that are configured in App Net Manager, do the following:

1. Expand the **Global Intranet Settings** menu in the domain directory.
2. Expand **User Remote Access** and then expand **Mobile User Administration**.
3. Select **Mobile User Groups**.

The following fields display for each Mobile User Group:

Mobile User Group	Displays the name of the Mobile User Group.
Number of Members	Displays how many Mobile Users belong to the Mobile User Group.

10.4.2.2 Add a Mobile User Group

Select **Mobile User Groups** and click the **New** button.

The Add Mobile User Group window will be displayed. On this window, fill out the fields as follows:

- **Mobile User Group Name:** Enter a name for the new Mobile User Group. The name of the Mobile User group must be unique, and cannot have the same name as a Client Group.

When you have finished filling out this window, click **OK** to save your changes. Click **Cancel** to cancel adding the new Mobile User Group.

Once you save with the **Save** button in the App Net Manager tool bar**,** your new Mobile User Group will appear in the list of Mobile User Groups. To add members to a group, select that group while adding or editing a Mobile User account with the **Mobile Users** feature.

10.4.3 Managing Legacy Corente Clients

Prior to this release, Corente Clients were created and managed using the **Client Administration** feature of Net App Manager. This section includes topics for managing legacy Corente Clients.

10.4.3.1 Managing a Legacy Corente Client Account

Note

From this release, you cannot add new accounts for legacy versions of the Corente Client. However, you can still edit legacy Corente Client accounts.

Legacy Corente Client accounts are managed using the **Client Administration** category in the domain directory. When you open the **Clients** subcategory, the domain directory lists each Client account you have configured. When you open a Client account, all the Client Groups of which it is a member will be displayed. For more information about Client Groups, see Section 10.4.3.2, “Add a Client Group”.

When you select **Clients**, all Corente Client accounts that have been configured in this domain will be displayed in a table to the right of the domain directory. This table displays:

- **Client:** the Client account name

- **Version:** the version of the software that the user has downloaded
- **Target:** the target software version that has been set for the user by the SCP Operator
- **Created:** the date that the Client account was created
- **Expires (Days):** number of days until the Client account expires. A value of Never indicates that No Expiration has been set for the Client account.
- **First Contact:** the first time the account contacted the SCP for activation
- **Last Contact:** the last time that the account connected and contacted the SCP
- **Visible IP:** the Visible IP address of the Corente Client

You can view the current status of each Corente Client at a glance in either the domain directory or the Clients table, by viewing the Corente Client's icon.

Icon	Status	Meaning
	Download	This account has been added by an administrator, but has not yet downloaded the Corente Client personality file.
	Downloaded	The Corente Client personality file has been downloaded, but the computer has not yet established a secure tunnel to the SCP.
	Active	The computer has established a secure tunnel to the SCP and is currently active on the Corente Services network.
	Disconnected	The computer has established a secure tunnel to the SCP at least once, but does not currently have a SCP connection. The Corente Client may not be in use.
	Upgrade Pending	When a purple triangle appears on the icon, the Corente Client is scheduled for a software upgrade.

You can **Edit** or **Delete** any existing Corente Client account. Once saved with the **Save** button in the App Net Manager tool bar, any changes made to an existing Corente Client will be distributed automatically and immediately if that Corente Client is currently connected. If the Corente Client is currently disconnected, the changes will be applied the next time the Corente Client contacts the SCP. If you delete a Corente Client currently in use, that Corente Clients session will be terminated.

To edit a legacy Corente Client account, right-click on the Client name in the domain directory.

The following settings are available:

- **Name:** Enter the alphanumeric identifier for the Corente Client account. You may use up to 50 alphanumeric characters. Hyphens and underscores are allowed, but do not use tabs, spaces, or punctuation marks when creating this name. This name must be unique from any Location names in your domain.
- **Email:** Enter the email address of the Corente Client user. The user will receive an email message shortly after you complete this screen, notifying them that you have set up this account. The email will also contain the URL where the user can obtain the Corente Client Software. If you have already downloaded the software, make sure you notify the user so that the user can obtain the software package from you rather than by using this hyperlink.
- **Password:** Create an alphanumeric password for this Corente Client account. This password must contain at least one uppercase, one lowercase, and one numeric character. This password will not be

sent in the automatic email message; for security purposes, you must supply the password to the user yourself. You should remind the user to change this password as soon as possible in order to maintain security for your domain.

- **Confirm Password:** Re-enter the password you created in the **Password** field to avoid any mistakes.
- **Notes:** If you would like to add additional information to keep track of this Client account, enter your notes here. You can enter up to 250 characters.
- **Access Settings:** The options in the **Access Settings** section allow you to select how this client account will use the Corente Client to connect to your Corente Services network.
  - **Allow access to local Network:** Select this option if you would like to allow the Corente Client to contact and be contacted by machines on its own LAN while it is connected to its Location partner. You should not select this option if this machine will be accessible by untrusted devices. When this option is *not* selected, while the software is in use, the Corente Client will only be able to contact and be contacted by machines via the Location partner. This option will be unselected by default.
  - **Backhaul All Traffic:** Select this option if you would like all traffic (both traffic destined for the Location partner and traffic destined for other places, such as the Internet) to travel inside the secure tunnel and be routed to the Location partner. The Location partner receives all of the traffic and then routes it appropriately. By default, this option will be selected. When this option is *not* selected, no traffic will be backhauled. This means that the Corente Client:
    - Is unable to use any WINS or DNS servers whose addresses have been served to it by a DHCP server over the domain (either by the Location gateway's DHCP server or by an external DHCP server).
    - Is able to access only the computers on the LAN of the Location to which it is connected.
    - Is unable to access the partners of its Location partner. The partners and computers behind those partners will be visible to the Corente Client user in Gateway Viewer, but will be inaccessible.
- **Authentication Type:** This section enables you to select the method that this Corente Client will use to authenticate to its Location partners. In addition to all of these methods, all Corente Clients are authenticated with digital certificates.
  - **Password:** Select this option and this Corente Client will authenticate with the user name and password that you supply on this screen. The password can be changed later by the user.
  - **External:** Select this option and this Corente Client will authenticate to its Location partner with either RADIUS or LDAP, depending on the type of external authentication that has been enabled on the Location gateway (see Section 11.9.9.3, "Configuring External Authentication"). The user must supply the user name and password that you have entered on this screen to obtain the personality file for this client, but must use the user name and password for the RADIUS/LDAP server to connect to the client's Location partner.

    Note

    If no External Authentication server has been enabled on the Location gateway, the Corente Client will be unable to connect to the Location when its **Authentication Type** is **External**.
  - **No Authentication:** Select this option and this Corente Client will not be required to authenticate with any other method but digital certificates. The user must supply the user name and password that you have entered on this screen to obtain the personality file for this client, but a user name and password will not be required when starting the software.

- **Client Expiration:** If you would like to create a temporary Client account for a user, you can use the **Client Expiration** feature to specify the length of time (in days) that the Client will be permitted to connect to its partners. When the subscription period has ended, the Client will immediately be disconnected by the SCP when the user attempts to start up the Client software and connect to partners. An expired Client account will remain listed in App Net Manager so that you are able to modify the **Client Expiration** settings and renew the Client subscription, easily rendering the Client account usable again.

  - **No Expiration:** When this option is selected, the subscription for this Client will not expire. The Client will be permitted to connect to its partners until you delete this Client account or change the **Client Expiration** settings. By default, this option will be selected.

  - **Expires In:** When this option is selected, the Client subscription will endure for the time period that is specified in the adjacent field. When the end of the time period approaches, the Client user will be notified of the impending expiration during initial Client startup. (The user can also view the length of time until client expiration at any time by placing their cursor over the Client system tray icon to view the 'tool tip'.) When the time period has ended, this Client will no longer be permitted to connect to its assigned partners until you change the **Client Expiration** settings. The default time period is 30 days.

  - **Expired:** When this option is selected, the subscription for this Client has expired. The Client will not be permitted to connect to its assigned partners unless you renew the subscription by selecting either the **No Expiration** or **Expires In** option and save your changes.

- **Client Group Assignments:** Corente Clients are combined into groups to make partner administration easier. Client Groups are created using the **Client Groups** feature, as described in Section 10.4.3.2, “Add a Client Group”.

  To include a Corente Client in a group, select the checkbox beside the group name. You may add a Corente Client to as many groups as you would like. A Client Group may contain up to 100 Corente Clients.

  If a Corente Client is member of multiple groups or partnered with multiple Location partners, when the user signs onto the service, they are asked to select a Location for that session. Corente Clients can connect to only one Location at a time.

  Note

  Corente Clients cannot be partnered with each other. Additionally, Corente Clients can only partner with Locations that are reachable on TCP or UDP port 551. This means that a client cannot connect to any Location behind firewall or proxy server unless that device has been modified appropriately.

10.4.3.2 Add a Client Group

Corente Clients are combined into groups to make partner administration easier. When you select **Client Groups** in the domain directory, all Client Groups that have been configured in this domain will be displayed in a table to the right of the domain directory. This table displays the Client Group names and the number of members of each group.

To view the members of an existing Client Group, open the Client Group's branch in the domain directory.

You can **Delete** any Client Group in this list. If the group is currently in use by any Corente Client, the Corente Client will no longer be able to contact any Locations partnered with that group.

To create a new client group, make sure **Client Groups** is selected in the domain directory and:

- Select the **New** button in the tool bar.

- From the **File** menu, select **Add Client Group**.
- Right-click **Client Groups** in the domain directory and select **Add Client Group**.

You will be taken to a blank **Add Client Group** window.

Fill out this window as follows:

- **Client Group Name:** Enter a new group name and click **OK**.

Once you save with the **Save** button in the App Net Manager tool bar, your new Client Group will appear in the list of Client Groups. To add members to a group, select that group while adding or editing a Corente Client account with the **Clients** feature.

10.4.3.3 Network Tab – Backhaul

A Corente Client can participate in the Corente Services backhaul feature. All IP traffic (both Internet and Corente Services network) from a Corente Client must be backhauled to its host Location across the secure Corente Services network tunnel. The "split tunnel" model (where the Corente Services network traffic is sent across the tunnel and the Internet traffic is sent directly to the Internet) can be enabled for specific Corente Client accounts, but it is generally recommended that all Corente Clients are backhauled. For more information about enabling or disabling backhaul for a legacy client, see Section 10.4.3.1, “Managing a Legacy Corente Client Account”.

Each Corente Services Gateway that is enabled for Mobile Users must function as a **Backhaul Server**. When you select the **Enable Client access to this Location** option, the Location form will automatically enable the **Backhaul Server** option as well. To verify backhaul settings, go to the **Network** tab and review the **Backhaul** section. The **Backhaul Server** option should be selected.

When the **Backhaul Server** option is selected, in addition to receiving the backhauled traffic of its Corente Client partners, the Location gateway can also receive backhauled IP traffic from Locations designated as **Backhaul Clients**.

If you would like, you can use the following option:

Optional Default Gateway: When the **Backhaul Server** option is selected, you can supply an IP address or DNS name of a server on the LAN where this Corente Services Gateway will send all of the Internet traffic that has been routed to it. This enables you to specify the server that the traffic will be sent to and received from for filtering and Internet access rules, so that you do not have to change the default Internet **Gateway** for this Corente Services Gateway in the **Network Interfaces** section of the **Network** tab.

Note

Because of backhaul, Corente Clients will access the Internet through their host Location when connected to the Corente Services network. Therefore, you must make sure that the appropriate configuration is completed on Corente Clients so that they can access the Internet at that location. In particular, if your users in your host Location’s site have to employ a proxy setting to reach the Internet, Corente Client users will also have to employ that same proxy setting because Internet access for the client is being backhauled through the office tunnel.

Under normal circumstances, to protect the Corente Services network, the Corente Client will not be able to communicate outside the Corente Services network tunnel. This means that all communication between a Corente Client and its own local network to which it is actually connected, such as a small Home network, is blocked while it is bridged to the LAN of its host Corente Services Gateway. However, when you configure a Corente Client account, you can select the **Allow access to the local network** option. When this option is selected, this Corente Client will be allowed to access computers on its own

LAN **in addition** to computers across the Corente Services network on the host Location's LAN. However, the Corente Client's Internet traffic will *not* be backhauled.

10.4.3.4 DHCP Server for Legacy Corente Clients

When connected to the Corente Services network, legacy Corente Clients must be provisioned by a DHCP server located on the LAN of their host Location. The DHCP server must serve each of the Corente Clients an IP address, network mask, and default gateway address, as well as DNS server and WINs server settings. You will not be able to create reservations for Corente Clients based on MAC address, since the MAC address used over the Corente Services network is not the actual MAC address used in each physical client machine. Instead, the MAC address is obtained via proxy.

A DHCP server simplifies administration of remote access clients enormously. Because it provides an IP address on the same subnet as the Location gateway, it enables users to access and use resources exactly as they would if their machine was plugged into the LAN itself. All of the domain security functions for users at work, such as logon scripts and automatic drive mappings, will now work easily over the Corente Services network connection for remote access users.

If you are already using a third-party DHCP server to provision computers on the Location gateway's LAN, you should also use this server to provision Corente Clients. However, if you do not have a DHCP server on the Location gateway's LAN, the Corente Services Gateway itself can be configured to handle this task for Corente Clients.

The address assignments served by the native DHCP server on the Location gateway will last for the duration of the Corente Client session while it is connected to this Location.

Perform the following steps to configure how addressing information will be served to Corente Clients on the **Edit RAS Client DHCP Server** screen of the Location form.

1. On the **User Remote Access** tab of the Location form, select the **DHCP Server Support Configure** button. The **Edit RAS Client DHCP Server** screen will be displayed.
2. Select the **Enable RAS Client DHCP Server** option to enable the DHCP server for Corente Clients.
3. If you would like, enter a **DNS Suffix** to be served to computers by DHCP. When these computers submit a name for DNS name resolution, this DNS suffix will be appended to that name.
4. Select either of the following options, if you would like:
   - **Serve DNS with DHCP:** This option enables you to select whether or not to pass DNS Server IP addresses with the DHCP leases. When this box is selected, Corente Clients will be served the DNS server addresses that you supplied in the **Network** tab of this Location form.
   - **Serve WINS with DHCP:** This option enables you to select whether or not to pass WINS Server IP addresses with the DHCP leases. (WINS is the network protocol used in Windows networking; the computer names you see in Network Neighborhood are all resolved into IP addresses, and vice versa, using WINS.)

     When this box is checked, you must enter the IP addreses of the WINS servers on your network that will be served to Corente Clients:

     - **Primary WINS:** Enter the IP address of the primary WINS server used to resolve WINS names on your local network.
     - **Secondary WINS:** Enter the IP Address of the secondary WINS server that will be used to resolve names if the primary WINS server does not respond. You cannot enter a Secondary WINS address if you have not entered a Primary WINS entry.

Note

When creating a Corente Client account, if the **Backhaul All Traffic** option is not selected, the Corente Client will not receive WINS and DNS server addresses when served its IP address by DHCP.

5. When you select the **Address Ranges** tab at the bottom of the screen, this section enables you to create the address pools that will be served by the Location gateway. You can **Edit** or **Delete** any existing range in this section. To begin creating address pools for Corente Clients, select the **Add** button.
6. The **Add DHCP Address Range** window will be displayed.

   Fill out this window as follows:

   - **Include Address Range** or **Exclude Address Range:** To start, make sure that the **Include Address Range** option is selected. This option indicates that the entire range you enter will be served by DHCP.
   - **Start Address:** Enter the lowest value of the address range in this field.
   - **End Address:** Enter the highest value of the address range in this field. If the address pool you would like to create contains only one IP address, you do not have to enter anything in this field.
7. Select the **OK** button to save this pool. The range will be listed in the **Address Ranges** section.
8. If you would like to *exclude* certain addresses from any of the address pools you have added, you can exclude these addresses by **Adding** another range and selecting the **Exclude Address Range** option. Then, enter the range of IP addresses that you would like to exclude in the **Start Address** and **End Address** fields, as described in **Step 6**. The address of the Location gateway is automatically excluded and does not need to be entered here.
9. Complete **Steps 5 to 8** to enter as many address ranges as you would like the Location gateway to serve.
10. When you select the **Reservations** tab at the bottom of this screen, you can reserve specific IP addresses for Corente Clients that receive their addressing from the Location's DHCP server. You can **Edit** or **Delete** any existing reservation in this section. To add a reservation, select the **Add** button.
11. The Add DHCP Reservation screen will be displayed.

    Fill out this screen as follows:

    - **Client Name:** Enter the name of the Corente Client.
    - **IP Address:** Enter the IP address that will be reserved by the Location's DHCP server for use by this Corente Client only. The Client will always receive this address from the DHCP server.
    - **Reserved:** When this checkbox is selected, the IP address you entered will be saved and assigned to the Corente Client whenever it receives its addressing via the Location's DHCP server.
12. Select the **OK** button to save this reservation. The range will be listed in the **Reservations** section.
13. Complete **Steps 10 to 12** to enter as many reservations as you would like the Location gateway to serve.
14. When you have finished defining the address ranges and reservations to be served by DHCP, click the **OK** button. You will return to the **User Remote Access** tab.

Chapter 11 Configuring and Monitoring Locations

Table of Contents

Locations are geographical sites in your Corente Services network where a Corente Services Gateway is running. When you install a Corente Services Gateway, you must add and configure a new Location in App Net Manager. After you set up the Location, you can modify the configuration and monitor the Location status in App Net Manager.

11.1 Creating Locations

You can add new Locations to your Corente Services network as follows:

- If you are adding a new Location for the first time, do the following:

  1. Select **File** then **Wizards** and then select **Location**.

     The **Add Location** wizard displays. This wizard guides you through the process of creating a new Location. You specify the minimum configuration settings for the Location to quickly add it to your network. You can edit the configuration after you complete the steps in the wizard, if required.

  2. Complete each step of the **Add Location** wizard and then click **Finish** when you successfully add the new Location.

  3. Select **File** and then **Save** to save your changes to the Corente SCP.

- If you have already added a Location to your Corente Services network, you can do the following:

  1. Select **File** then **Add Location**.

     The **Add Location** window displays.

2. Configure settings on the **Add Location** window as appropriate and then select **OK**.
3. Select **File** and then **Save** to save your changes to the Corente SCP.

After you successfully create a new Location, you must download the configuration file to the Corente Services Gateway.

Related Information.

- Section 11.9, “Settings on the Location Window”
- Section 11.4, “Downloading Location Configuration Files”

11.2 Editing Locations

You can edit the configuration of a Location at any time. You cannot change the name of the Location but you can change any other configuration setting.

To edit a Location, do the following:

1. Expand the **Locations** folder in the domain directory.
2. Select the Location you want to edit and then right-click and select **Edit**.

   The **Edit Location** window displays.
3. Configure settings on the **Edit Location** window as appropriate and then select **OK**.
4. Select **File** and then **Save** to save your changes to the Corente SCP.

After you save changes, the Corente Services Gateway automatically retrieves the new configuration from the Corente SCP, if you have already downloaded the configuration file to the Corente Services Gateway. In some cases, configuration changes require the Corente Services Gateway to restart, which temporarily interrupts the Corente Services network for that Location.

11.3 Deleting Locations

You can delete Locations from your Corente Services network, as follows:

1. Expand the **Locations** folder in the domain directory.
2. Select the Location you want to delete and then right-click and select **Delete**.

   The **Delete Location** dialog displays.
3. Enter your administrator password to confirm that you want to delete the Location.

App Net Manager deletes the entire Location from your Corente Services network. The Corente Services Gateway and all computers behind it no longer connect to the Corente Services network.

11.4 Downloading Location Configuration Files

When you install the Corente Services Gateway and create a new Location in App Net Manager, you must download the configuration file to the Corente Services Gateway.

Note

If you use **Zero Touch Configuration** you do not need to download the configuration file. The Corente Services Gateway automatically retrieves it through

the Corente SCP. See the *Corente Services Gateway Deployment Guide* for more information.

Important

Corente Cloud Services Exchange recommends that you keep a backup copy of the Location configuration file after you download it. You can quickly restore Locations with the backup copies of the configuration files in the event you need to reinstall Corente Services Gateways or recover from hardware failures.

To download a Location configuration file, do the following:

1. Select **File** then **Wizards** and then select **Download Location**.

   The **Download Location Configuration** wizard displays. This wizard guides you through the steps to download the configuration file for a Location.

2. Complete each step of the **Download Location Configuration** wizard and then click **Finish** when you successfully download the configuration file.

11.5 Duplicating Locations

You can duplicate a Location to quickly create new Locations with similar configurations, as follows:

1. Expand the **Locations** folder in the domain directory.
2. Select the Location that you want to duplicate and then right-click it and select **Duplicate**.
3. Select the Location that you want to duplicate and then right-click it and select **Duplicate**.

   The **Duplicate Location** dialog displays.

4. Select **Yes** to duplicate the Location.
5. Specify a name for the new Location.

   App Net Manager creates a new Location using the configuration settings of the Location that you duplicated.

6. Select the new Location from the **Locations** folder and then right-click it and select **Edit**.

   The **Edit Location** window displays.

7. Modify the Location configuration as appropriate and then select **OK**.
8. Select **File** and then **Save** to save your changes to the Corente SCP.

Related Information.

- Section 11.9, “Settings on the Location Window”
- Section 11.4, “Downloading Location Configuration Files”

11.6 Scheduling Upgrades

By default, Corente Services Gateway software upgrades occur automatically in the preferred maintenance time that you specify on the **Location** tab on the configuration window for Locations. You can schedule upgrades to change the date and time when the Corente Services Gateway software upgrade occurs.

1. Expand the **Locations** folder in the domain directory.

2. Select the Location for which you want to schedule an upgrade.

> **Note**
>
> A purple triangle icon displays for Locations when a software upgrade is available: .

3. Right-click the Location and select **Schedule Upgrade**.

   The **Schedule Upgrade of Location** dialog displays.

4. Specify upgrade details for the Location, as follows:

   - **When** specifies one of the following options:
     - **First Maintenance Time after** schedules the upgrade to occur in the first maintenance window after the date that you schedule.
     - **As soon as possible after** schedules the upgrade to occur at the first available time after the date that you schedule.
   - **Local Time** lets you specify a local system date and time for the upgrade to occur.
   - **Location's Time** lets you specify a date and time that is local to the Corente Services Gateway host computer.

     > **Note**
     >
     > If you specify a date and time in the past, the software upgrade occurs as soon as possible.

   - **Reset To** lets you select one of the following options to restore date and time for the upgrade:
     - **Now** resets to the current date and time.
     - **Week** resets to the date and time one week ahead of the current date and time.
   - **Administered Weekly Maintenance Time** displays the preferred maintenance time that is set in the Location configuration.
   - **Password** specifies your App Net Manager password to schedule the upgrade.

5. Select **Upgrade** to save the changes to the upgrade schedule.

The Corente Services Gateway software upgrades according to the date and time you scheduled for the Location. For the software upgrades to occur, Locations must be active and connected to the Corente SCP.

11.7 Generating New Encryption Keys

Corente Services Gateways use encryption keys to establish secure connections with the Corente SCP and to create secure tunnels with other devices on your Corente Services network.

> **Important**
>
> Generating new encryption keys temporarily interrupts service while the Corente Services Gateway re-establishes secure connections with devices on your Corente Services network.

You can generate new encryption keys for Corente Services Gateways as follows:

1. Expand the **Locations** folder in the domain directory.
2. Select the Location for which you want to generate a new encryption key.
3. Right-click it and select **Regenerate** and then select **Key**.

   The **Regenerate Location Key** dialog displays.
4. Enter your App Net Manager password and then select **Generate**.

11.8 Generating New Configuration Files

If a Location is disconnected or inactive, you can generate a new configuration file to download and install on to the Corente Services Gateway.

You can generate new configuration files for Corente Services Gateways as follows:

1. Expand the **Locations** folder in the domain directory.
2. Select the Location for which you want to generate a new configuration file.
3. Right-click it and select **Regenerate** and then select **Configuration**.

   The **Regenerate Location Configuration** dialog displays.
4. Enter your App Net Manager password and then select **Generate**.

You must now install the configuration file on the corresponding Corente Services Gateway. See the *Corente Services Gateway Deployment Guide* for more information.

11.9 Settings on the Location Window

You specify settings on the **Location** window to configure Corente Services Gateways.

11.9.1 Location Tab

The Location tab captures basic information regarding your new site.

Identity and Location

This section captures information regarding the name and physical location of your new site.

Location Name: Enter the alphanumeric identifier for the Location that you are creating. This name must be unique within your domain. This name cannot be changed once you complete this form, so choose carefully. This will be the name used at all times to identify this Location, and will be assigned as the actual computer name of the Corente Services Gateway when it is booted with the configuration file that you are currently preparing. If you choose a name that is a valid NetBIOS name (i.e., 15 characters or less), users can connect to the Location to access remote computers on the domain using this name instead of the IP address.

Street Address: Enter the street address of the new Location that you are creating. This address can be up to 100 alphanumeric characters.

City: Enter the name of the city where this Location will be located. You may use up to 30 alphanumeric characters for this field.

State/Province: Select the appropriate state or province from the pull down list provided.

Postal Code: If applicable, enter the 5 digit U.S. postal code for the location of this Location. The initial placement of your Location icon on the U.S. map will be determined by this zip code. If you do not enter a valid code in this field, the icon will be placed in the upper right hand corner of the map.

Country: Select the appropriate country from the pull down list provided.

Time Zone: Select the appropriate time zone for the Location from the pull down list provided.

Maintenance

This section captures information regarding the upgrade preferences for this Location.

Require Administrator approval to enable Partner connections: By checking the box, you will require that the Corente Services Gateway is approved by an administrator before it is fully operational. When this option is selected for a new Corente Services Gateway and the configuration file for the Corente Services Gateway is downloaded, the new Location gateway is active but unable to connect to any of its partners. However, it is in communication with the Corente SCP while it waits for approval, so that connection to its partners can begin immediately following approval. The gateway icon is marked with a black triangle to signify that approval is required.

To approve the Corente Services Gateway, an administrator must right-click the Corente Services Gateway's icon in App Net Manager and select **Approve Partner Connections**. The Approve Partner Connections window will be displayed. Enter your login password and click Approve to approve the connections. Approval will be required again if the configuration is ever regenerated and re-downloaded. By leaving the box unchecked, the Corente Services Gateway will become operational and connect to its partners immediately following configuration download.

Automatic reboot after maintenance: Leave this box selected if you would like your Corente Services Gateway to automatically reboot after maintenance has been performed. If this box is selected, be aware that a reboot will pause your network connections until the operation is complete. If you unselect this box and your software has been upgraded, you will have to manually reboot the Corente Services Gateway in order for the machine to switch to the upgraded software. By default, this option is selected.

Preferred maintenance time: Upgrades to new versions of the Corente Services Gateway software will occasionally be downloaded automatically to your Location gateway from the Corente SCP. Select a day of the week and an hour when your network is least busy so that it can be interrupted for these upgrades safely, without harm to your business.

Remote Logging

This section allows you to specify a server that will capture log messages from the Corente Services Gateway. These options require the logging server to be configured appropriately to accept a syslog feed.

System Logging: Select this option to send all system log messages to an external server. The system log is normally recorded on the Corente Services Gateway itself. However, when this option is selected, the Location gateway will track and send all firewall log events to be recorded on the logging server that you specify. This is a traditional firewall log; a message is sent whenever a packet is denied from passing through the Corente Services Gateway. When this option is selected, the Logging Server Address field must be filled in.

Logging Server Address: When system logging is selected, enter the IP address of the logging server in this field. All log messages will be sent to this server.

Redundant Hardware Configuration

This section captures your preferences if you would like to provide redundant hardware for this Corente Services Gateway configuration. Hardware redundancy provides a site with a backup domain connection to

use in the event of a hardware or software failure of the site's active Corente Services Gateway. To provide backup, two servers loaded with the Corente Services Gateway software are installed on the LAN. These servers function as a single entity, each alternating between serving as the Active Location gateway and the Standby Corente Services Gateway. You will not be able to choose which Corente Services Gateway is Active and which is Standby; this is negotiated between the pair.

Redundant hardware requires each participating Corente Services Gateway server to have an additional, dedicated Ethernet interface. (This means that Corente Services Gateways using the Peer configuration must have at least two Ethernet cards, and gateways using the Inline configuration must have at least three Ethernet cards.) The two gateways will be connected via these Ethernet interfaces. You can do this using either a VLAN on a router or a dedicated hub. The Ethernet interfaces for the two Location gateways will be on their own subnet (1.1.1.1/30).

The Active and Standby Corente Services Gateways require only one configuration file to be used between them. The Location gateways must both be connected to the LAN and to the same Internet Access Device, and share a set of IP address(es) and MAC address(es) for their LAN and WAN (or LAN/WAN) interface(s). The configuration file must be manually installed on the first Corente Services Gateway. Make sure a monitor/keyboard or is connected to this server. Also ensure that the router or hub to which the two Locations gateways will connect is turned on. When the first Corente Services Gateway reboots, the installation interface will ask to identify the MAC address of the backchannel port being used for redundant hardware:

```
"This is to configure the backchannel network interface port for the hardware
failover. Now please disconnect all network cables to this gateway machine.
Identify the network port that is dedicated to the hardware failover. Using a cable,
connect the dedicated port to a hub, switch, or an active network device. Make sure
you see the 'link' light of the network port is on. Select 'Continue' to continue with
the Backchannel Configuration."
```

After following these directions, make sure both servers are connected to the LAN, hub or router, and have access to the Internet. Next, the software should be loaded onto the second server. Make sure a monitor/keyboard is connected to this server. This server will reboot, and the Failover Configuration option must be selected on the installation interface. The configuration will then load onto the second server, and the installation interface will ask to identify the MAC address for this server as well.

Note

If you have enabled the Dual WAN feature on the Network tab, you will be unable to enable hardware failover.

When a software upgrade occurs (during the maintenance window that you scheduled above), the Corente Services Gateway hardware that is currently Active will be upgraded first. Once the upgrade has completed, the hardware will alternate and the Standby Location gateway will become Active so that it can be upgraded as well. This may cause multiple upgrade and tunnel up/tunnel down alerts, because the Corente Services Gateway that is upgraded first will attempt to re-establish its tunnels before the hardware switch occurs. Before it becomes the Standby Corente Services Gateway, it will bring the tunnels down again. Once the second Corente Services Gateway has completed the upgrade, it will establish the tunnels and remain as the Active Corente Services Gateway until the next hardware switch occurs.

Enable Redundant Hardware configuration: Select this option to enable hardware redundancy. If this option has been enabled, the following additional options will be available:

Enable scheduled hardware switch during weekly maintenance window: Select this option if you would like the Corente Services Gateways to rotate weekly between which Corente Services Gateway is designated as the Active and which as the Standby, so that each piece of hardware can be regularly confirmed to be functioning correctly. This switchover will occur during the weekly Preferred maintenance time that you specified above.

The following settings allow you to specify the timing of the failover intervals:

Redundant Hardware Keep-Alive Interval (seconds): The interval of time between each "heartbeat packet" that is sent by the Standby Corente Services Gateway to the Active Corente Services Gateway to make sure that the Active Corente Services Gateway is still functioning. The default is 60 seconds, with a maximum of 600 seconds.

Failover Interval after loss of Keep-Alive (seconds): The period of time that the Standby Corente Services Gateway will wait to initiate failover if the Active Corente Services Gateway has not responded to its "heartbeat" packet. This variable must be set at least twice the amount of time as the Redundant Hardware Keep-Alive Interval; therefore, the default is 120 seconds, with a maximum of 1200 seconds.

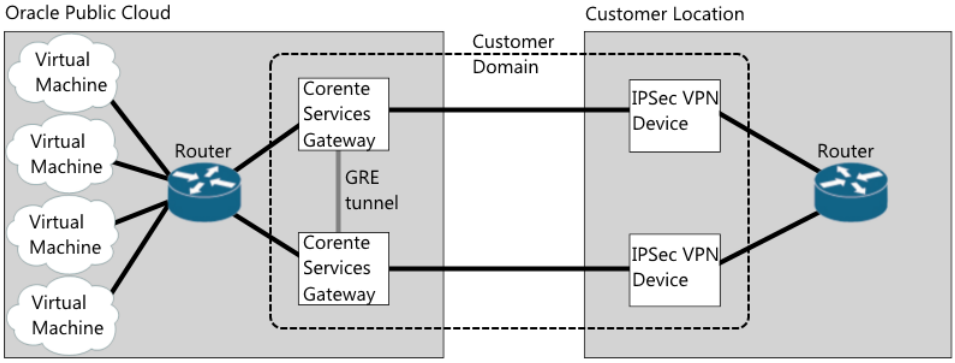
Every 10 attempts, the Redundant Hardware Keep-Alive Interval will be doubled, maxing out at 600 seconds. If this makes the interval longer than the Failover Interval after loss of Keep-Alive, then that interval will be doubled as well, maxing out at 1200 seconds. Upon success (or a restart after a failover), both intervals will revert back to the initial configured time.

Cloud Failover

The **Cloud Failover** section is available if you use a supported third-party VPN device configuration and applies only in the Oracle Public Cloud environment.

Failover Location Address: Specifies the LAN IP address of the Corente Services Gateway you plan to use as a failover location. In the event that the IPSec tunnel to the third-party device becomes unavailable, the Corente Services Gateway forwards packets to the failover location. The failover occurs within 30 seconds.

The following diagram illustrates the cloud failover configuration:



The preceding diagram shows two Corente Services Gateways that reside on the Oracle Public Cloud network and two third-party VPN devices that reside on the customer network. You configure the Corente Services Gateways and the third-party VPN devices on the same domain in App Net Manager. The two Corente Services Gateways are not partners. You partner each Corente Services Gateway with one of the third-party VPN devices.

In a cloud failover configuration, Corente Services Gateways:

- Must have an inline configuration.
- Must have the same LAN configuration. Although Corente Services Gateways do have different LAN IP addresses.
- Must have the same User Group configuration.

You must enable dead peer detection (DPD) for the third-party VPN devices and ensure that they have the same subnet configuration.

Zero Touch Configuration

This section captures your preferences for Zero Touch Installation, which allows you to install a new Corente Services Gateway simply by placing a server loaded with the gateway software on the network and turning it on. When installing a new Location gateway, the configuration file is downloaded upon the first reboot after software installation. If there is no configuration file found on a floppy, a USB, or on the hard drive, the new Corente Services Gateway will attempt to acquire a dynamic IP address via DHCP.

To utilize Zero Touch Installation, the Corente Services Gateway must be able to connect to the Internet, and the DNS server must be able to resolve `www.corente.com`to the Corente SCP. Communication between the new Corente Services Gateway and the Corente SCP is secured using the HTTPS protocol.

Zero Touch Installation cannot be used when the following IP addressing options are used for the WAN (Inline configuration) or WAN/LAN (Peer configuration) interfaces of the Location gateway:

- Static IP address
- PPoE
- Proxy Server

Note

These options may be used for normal operation of the Location gateway, however they cannot be used to download the configuration via Zero Touch Installation.

Fill out the fields as follows:

Enable Zero Touch Configuration: Select this option to enable Zero Touch Configuration.

Unique Identifier: Enter the unique identifier for the Corente Services Gateway server. You need only enter one unique identifier: either a service tag or a MAC address of one of the Corente Services Gateway's Ethernet interfaces. The software reads the service tag and all MAC addresses from the Corente Services Gateway server and passes all of them to Corente SCP, which then matches the identifier with the appropriate configuration file.

Notes

This field allows you to save notes about this Location that can be viewed by other administrators of the domain. You can enter up to 250 characters.

Advanced Performance Tuning

You can disable the options in this section to improve the throughput of the gateway by suppressing potentially compute-intensive side processes.

Enable Probe Monitoring (Security): Select this option to enable the Location gateway to determine if hostile network probing is occurring through the network. When deselected, probe monitoring is disabled and notifications will not be sent.

Enable Report Data Collection: Select this option to enable the collection of data for reports and graphs, such as bandwidth reports. When deselected, the gateway does not collect and present this data in App Net Manager.

Enable Compression: Select this option to enable compression for IPSec connections. Turning compression off on high-speed links results in better throughput performance. By default, compression is disabled for a new Location.

11.9.2 Network Tab

The Network tab captures the following network-specific IP address information:

11.9.2.1 Network Interfaces

This section enables you to modify the network addresses that were assigned to the Ethernet interfaces of this Location gateway. All addresses that have been defined for the Ethernet interfaces of the Corente Services Gateway are listed in the table in this section.

To add a new network interface to this list, select the **Add** button. You can also **Edit** or **Delete** an existing interface. When Add is selected, you must select the type of configuration that your Corente Services Gateway will use and the interface that you want to define.

Peer Configuration

The Peer configuration is a Corente Services Gateway with a single Ethernet interface. The Peer Corente Services Gateway is added to an already existing LAN consisting of the machines that will be participating in the application network. It requires additional routing or server configuration to ensure that packets destined for a partner Location get routed to the local Corente Services Gateway first.

If your Corente Services Gateway is a Peer, select the **WAN/LAN interface** option and click **OK** to add or edit the interface.

Addressing and DNS: You supplied your addressing and DNS preferences using the Location Wizard. These preferences are shown in this window, but can be changed at any time.

GRE Tunnels: This window enables you to configure use of a GRE (Generic Routing Encapsulation) tunnel for the LAN. Select the Use GRE Tunnel checkbox and enter the IP address for the tunnel.

Note

IP addresses in the 10.x.x.x range are not supported for GRE tunnels.

Proxy Server: This window enables you to indicate whether or not a proxy server is installed between this Corente Services Gateway and the Internet. There are two types of proxy supported, SOCKS and Web.

- **Internet Access via Proxy Server:** Check this box if your Location gateway connects to the Internet from behind a proxy server.
  - **Proxy Type:** In the drop-down list, select SOCKS or Web. Select SOCKS if your proxy server provides SOCKS V4/V5 server support in order to interoperate with the Corente Services Gateway. When this is selected, the Proxy IP Address and Port fields will be enabled and must be filled in. If the proxy server is a web proxy, select Web and the Proxy IP Address and Port fields will be enabled and must be filled in.

- **Proxy IP Address:** If you check Internet Access via Proxy Server, enter the IP address of the proxy server that your Corente Services Gateway operates behind. Even if your Corente Services Gateway is a DHCP client, you must determine the address of the proxy and enter it here.
- **Proxy Port:** If you check Internet Access via Proxy Server, you must enter the port number that your proxy server uses. This must be specified to allow the automatic Corente Services Gateway software updates to occur on your Corente Services Gateway. The default port is 80, which is used by most proxy servers.

Important

Additional configuration is required when your LAN includes a proxy server. You must make sure that all the computers on the same subnet as your Corente Services Gateway change the settings of their web browser to bypass the proxy server for local addresses and to specifically exclude the IP Address of the Corente Services Gateway.

Similarly, if you need to access the App Net Manager from a computer operating behind a proxy server, you must exclude the address of this application in your browser as well.

For example, if you are using Internet Explorer and you are operating behind a proxy server:

1. Select the **Tools** menu and choose **Internet Options**.
2. In the new window that opens, select the **Connections tab**.
3. Click the **LAN Settings** button when it appears. Make sure that the Use a proxy server checkbox is marked.
4. Enter the LAN IP Address and port number of the proxy server in the fields provided, and then make sure that the **Bypass proxy server for local addresses** checkbox is selected.
5. Click the **Advanced...** button right next to these fields and enter the IP Address of your Corente Services Gateway in the Exceptions list. Traffic destined for App Net Manager at `https://www.corente.com/appnet` should not be routed to the proxy server, either. If you are granting access to the App Net Manager application, enter the address `https://www.corente.com/appnet` into the Exceptions list as well.
6. Click **OK** twice and your browser settings will be stored.

Important

This process **must** be performed on each computer's web browser in order for the computers to access the Corente Services Gateway and application network.

DHCP Servers: This window enables you to configure the Corente Services Gateway DHCP server that can distribute IP addressing information to computers on the Corente Services Gateway's LAN, as well as to its Corente Client partners. click the LAN DHCP Server Configure button.

Interface Aliases: This window enables you to assign alias addresses to the LAN/WAN interface of the gateway. Alias addresses are used with the port forwarding feature, which directs traffic from the Internet/WAN through the gateway to servers on the LAN or in the DMZ.

Inline Configuration

The Inline configuration is a Corente Services Gateway with two Ethernet interfaces. One Ethernet interface is connected to the internal local area network (LAN). The other interface is connected to an external interface, which is typically the Internet access device for that location. All traffic must pass through the Corente Services Gateway in order to reach into and out of the internal local network.

If your Corente Services Gateway is an Inline, you must configure both a LAN and a WAN interface. You also have the option of configuring a secondary WAN interface, if you would like to use the Dual WAN feature, or a DMZ interface, if you will be using your Corente Services Gateway to implement a DMZ.

Addressing and DNS: You supplied your addressing and DNS preferences for both the LAN and the WAN interfaces in the Location Wizard. These preferences will appear each interface's window, but can be changed at any time.

GRE Tunnels: This window enables you to configure use of a GRE (Generic Routing Encapsulation) tunnel for the LAN. Select the Use GRE Tunnel checkbox and enter the IP address for the tunnel.

Note

IP addresses in the 10.x.x.x range are not supported for GRE tunnels.

DHCP Servers: The Edit LAN Interface window enables you to configure the Corente Services Gateway DHCP server that can distribute IP addressing information to computers on the Corente Services Gateway's LAN, as well as to its Corente Client partners. Click the LAN DHCP Server Configure button.

Proxy Server: In addition to assigning addressing information, this window enables you to indicate whether or not a proxy server is installed between this Corente Services Gateway and the Internet. There are two types of proxy supported, SOCKS and Web.

- **Internet Access via Proxy Server:** Check this box if your Location gateway connects to the Internet from behind a proxy server.
  - **Proxy Type:** In the drop-down list, select SOCKS or Web. Select SOCKS if your proxy server provides SOCKS V4/V5 server support in order to interoperate with the Corente Services Gateway. When this is selected, the Proxy IP Address and Port fields will be enabled and must be filled in. If the proxy server is a web proxy, select Web and the Proxy IP Address and Port fields will be enabled and must be filled in.
  - **Proxy IP Address:** If you check Internet Access via Proxy Server, enter the IP address of the proxy server that your Corente Services Gateway operates behind. Even if your Corente Services Gateway is a DHCP client, you must determine the address of the proxy and enter it here.
  - **Proxy Port:** If you check Internet Access via Proxy Server, you must enter the port number that your proxy server uses. This must be specified to allow the automatic Corente Services Gateway software updates to occur on your Corente Services Gateway. The default port is 80, which is used by most proxy servers.

Important

Additional configuration is required when your LAN includes a proxy server. You must make sure that all the computers on the same subnet as your Corente Services Gateway change the settings of their web browser to bypass the proxy server for local addresses and to specifically exclude the IP Address of the Corente Services Gateway.

Similarly, if you need to access the App Net Manager from a computer operating behind a proxy server, you must exclude the address of this application in your browser as well.

For example, if you are using Internet Explorer and you are operating behind a proxy server:

1. Select the **Tools** menu and choose **Internet Options**.
2. In the new window that opens, select the Connections tab.
3. Click the **LAN Settings** button when it appears. Make sure that the **Use a proxy server checkbox** is selected.
4. Enter the LAN IP Address and port number of the proxy server in the fields provided, and then make sure that the **Bypass proxy server for local addresses** checkbox is selected.
5. Click the **Advanced...** button right next to these fields and enter the IP Address of your Corente Services Gateway in the Exceptions list. Traffic destined for App Net Manager at `https://www.corente.com/appnet` should not be routed to the proxy server, either. If you are granting access to the App Net Manager application, enter the address `https://www.corente.com/appnet` into the Exceptions list as well.
6. Click **OK** twice and your browser settings will be stored.

Important

This process **must** be performed on each computer's web browser in order for the computers to access the Corente Services Gateway and application network.

Interface Aliases: The Edit WAN Interface screen enables you to assign alias addresses to the WAN interface of the gateway. Alias addresses are used with the port forwarding feature, which directs traffic from the Internet/WAN through the gateway to servers on the LAN or in the DMZ.

WAN Secondary Interface

The Dual WAN feature allows customers to set up WAN failover for a Corente Services Gateway from a primary WAN connection to a secondary WAN connection, to ensure continued access to the secure Corente Services network and Internet in the event of a WAN failure. After failover, the gateway will detect when the primary WAN connection has recovered and will automatically failback. Note that this feature does not currently support load balancing across the two WAN connections.

The Dual WAN feature can be used with a Corente Services Gateway in the Inline configuration that contains at least three Ethernet cards. One Ethernet card is for the LAN connection, one is for the primary WAN connection, and one is for the secondary WAN connection.

Dual WAN cannot be enabled on a gateway that is using the following features:

- Hardware failover.
- WAN interface alias addresses for port forwarding on either the primary WAN interface or secondary WAN interface.

If you plan to enable Dual WAN for gateway already in use, it is recommended that you perform a new installation of the Corente Services Gateway Software and personality file on your hardware due to several

specific installation steps that are required. In particular, ensure that the gateway to which you are adding this feature is turned off before starting installation of the personality file.

To configure the secondary WAN interface, select **WAN Secondary Interface** on the Add Network Interfaces dialog box. In the Addressing section on the window that appears, select how an IP Address, Subnet Mask, and Default Gateway will be assigned to this secondary WAN interface.

- **DHCP:** Select this option to allow a DHCP Server to automatically assign an IP Address, Subnet Mask, and Gateway address to the secondary WAN interface of this gateway.
- **Static:** When this option is selected, you must manually enter addressing information for this interface.
- **PPPoE:** Select this option if your gateway will use PPPoE to connect to the secondary WAN connection from this interface.

In the WAN Failover section, fill out the field as follows:

- **Failover/Failback detection interval:** Enter the period of time (in seconds) that the gateway will wait before an outage of the primary WAN connection causes a failover to the secondary WAN connection. Once the primary WAN connection comes up again, failback will be delayed for the same interval or 300 seconds, whichever is less. This ensures that the primary WAN connection is operational and prevents flapping of the interface. The default failover interval is 600 seconds, but can be between 30 seconds and 86,400 seconds (24 hours). The default failback interval is 300 seconds, but will use the same interval you have set for the failover interval, up to a maximum of 300 seconds. Note that failover and failback will each cause a restart of the gateway service (but not of the gateway hardware itself).

After installing (or reinstalling) the Corente Services Gateway software onto your gateway, make sure the gateway hardware is turned off. Connect the Ethernet cable for the primary WAN to one of the gateway's Ethernet interfaces. It does not matter which Ethernet interface this cable is plugged into, as the gateway will itself designate that particular interface as the primary WAN interface. Do not connect the secondary WAN connection to an Ethernet interface yet.

Once the gateway has started up and connected to the Corente SCP over the primary WAN connection, connect the Ethernet cable for the secondary WAN connection to an Ethernet interface of the gateway. You should then access the Control page of Gateway Viewer and force a failover to the secondary WAN connection to ensure that it is working.

After you add a WAN Secondary Interface, the interface identified as WAN Interface will function as the primary WAN interface.

Enable Alias Addresses for Port Forwarding

Normally, a Corente Services Gateway prevents access to the LAN from the Internet/WAN, allowing external connections only from partner Locations or Corente Clients. But your corporate network may contain servers that must be reachable by Internet/WAN traffic. For example, a web server that serves your company's website. Port forwarding allows these servers to use the gateway's LAN/WAN or WAN interface as their own public interface, with the gateway filtering out the unwanted traffic and passing on only the approved type of traffic to the designated server.

Specifically, port forwarding allows an administrator to forward traffic bound for particular ports of the gateway's LAN/WAN or WAN address to the appropriate servers behind the gateway. For example, port forwarding can be configured so that all traffic pointed at the gateway's WAN address and port 80, the standard port used for HTTP traffic, is forwarded by the gateway to a web server in your DMZ.

If multiple DMZ servers will need to utilize the same port, an administrator can create multiple alias addresses for the gateway's LAN/WAN or WAN interface and ensure that all incoming traffic through the gateway to that alias address is forwarded to specific servers on the private LAN of the DMZ. Aliases are

used, for example, when you have two web servers in your DMZ that both use HTTP on port 80. One server can use the LAN/WAN or WAN address of the gateway as its routable address, but each additional server using port 80 will require a distinct routable address to ensure that traffic is routed appropriately. The addresses that you use as aliases must be routable addresses that are otherwise not in use.

To configure alias addresses, edit the LAN/WAN or WAN interface of the Corente Services Gateway. Click the **Add** button in the Interface Aliases section.

Fill out the fields as follows:

- **Interface Alias Name:** Enter a name for this alias. This name will be used for administration purposes in App Net Manager.
- **Alias IP Address:** Enter the alias IP address for the interface. The address that you enter here must be a routable address that is otherwise not in use.

  Click **OK** to save the alias. The alias will now be listed in the Interface Aliases section.

Click **OK** again when you have finished adding alias addresses. You will use the aliases you have entered to forward traffic from the gateway to the appropriate servers via tube definitions for the DMZ to Internet Access partner or LAN to Internet Access partner on the Partners tab of the Location form.

Port forwarding and aliases are not necessarily used only with a DMZ. They can also be used whenever you have multiple servers using the same port and you would like them all to be reachable from the Internet/WAN. These multiple servers may not reside in your DMZ, but directly on your LAN.

11.9.2.2 Backhaul

Backhaul is a feature that enables you to aggregate all of your application network locations' Internet traffic and have it exit outbound to the Internet and enter inbound to your network via either a single location, or multiple locations. Backhaul requires at least two active Locations in your Corente Services domain. One must be designated as a Backhaul Server and the other as a Backhaul Client.

A Corente Services Gateway that is administered as a Backhaul Client will encrypt all Internet traffic and send it to a Corente Services Gateway designated as a Backhaul Server. The Backhaul Server will route Internet traffic from these Locations to the Internet. This traffic will be routed through whatever devices exist on the Backhaul Server’s network to filter Internet traffic. All application network traffic will continue to use the appropriate tunnels for each partner.

- **No Backhaul:** This Location will not participate in backhaul. This is the default setting for backhaul.
- **Backhaul Client via server:** If you select this option, you must select a Backhaul Server from the selection box beside this option. All Internet traffic for this gateway's LAN will be routed to and from the selected Backhaul Server. Routers behind this Corente Services Gateway will need to be modified to send all outgoing Internet packets to the Corente Services Gateway. The Corente Services Gateway will then send the packets to the gateway designated as the Backhaul Server.
- **Backhaul Server:** This will be a Location to which the Locations designated as Backhaul Clients will send and receive Internet traffic.
  - **Optional Default Gateway:** When the Backhaul Server option is selected, you can supply an IP address or DNS name of a server that this Corente Services Gateway will send all of the Internet traffic that has been routed to it. This enables you to specify the server that the traffic will be sent to for filtering and other such services, so that you do not have to change the default Internet Gateway for this gateway in the Network Interfaces section of the Section 11.9.2, “Network Tab”.

If you enable Backhaul, it is important to define a Special Internal Network Description User Group on the User Groups tab that includes all IP addresses on the corporate network. This will allow the Corente

Services Gateway to distinguish between the Internet, subnets participating in the application network, and subnets not participating in the application network, so that traffic will not have the opportunity to be routed to the wrong location and create a security risk. For example, if a Special User Group is not defined, a Corente Services Gateway designated as a Backhaul Server might route non-application network traffic from a Backhaul Client to one of its own non-participating subnets, mistaking the subnet's address as part of the Internet.

If a subnet behind a Corente Services Gateway is on a public, world-routable public IP address space, then NAT must occur some place outside the Corente Services Gateway at the Backhaul Server site. If NAT does not occur, return packets will not flow back through the server and tunnels properly to the subnet.

11.9.2.3 RIPv2, OSPF, and BGP

Routing Information Protocol (RIPv2), Open Shortest Path First (OSPF), and Border Gateway Protocol (BGP) can be enabled on your gateway to automate routing if your LAN is divided into multiple subnets and you would like more than one of these subnets to participate in your Corente Services application network.

RIPv2, OSPF, and BGP are useful in environments where routes to these different subnets are changing dynamically. If you enable RIPv2, OSPF, and BGP, you do not need to add static routes for the subnets on the Routes tab of this Location’s Location form. However, you must have entries on the User Group screen for these subnets so that the machines on the subnets can participate in the application network. You must also make sure that there are routers on your local network that know about these subnets and you must configure the routers to respond to RIPv2, OSPF, and BGP.

RIPv2

RIPv2 is a protocol widely used for routing traffic. It is an interior gateway protocol (IGP), which means that it performs routing within a single autonomous system, such as the local area network (LAN). RIPv2 works by sending routing-update messages to computers on the LAN at regular intervals and whenever the network topology changes. RIPv2 identifies how routing on a network has changed by measuring the **hop** of a RIPv2 packet from its source to its destination. Each hop in a path from source to destination is noted and distributed. When a computer receives a RIPv2 routing-update that includes changes to an entry, it updates its routing table to reflect the new route.

The Corente Services Gateway will support RIPv2 multicast and unicast messages without authentication. The Corente Services Gateway does not support RIPv1 broadcast messages.

To enable RIPv2 on a gateway;, the RIP section on the Section 11.9.2, “Network Tab” of the Location form must be completed as follows:

- **Enable Routing Information Protocol (RIPv2) on LAN:** When this option is selected, the Corente Services Gateway will use RIPv2 to announce routes on the LAN that can used to reach remote application network subnets.
  - **Use non-standard default weight for RIP:** To use a non-standard default weight for RIPv2, select this option and enter the weight in the field provided. The default weight is 1. Valid values for this option are 1 to 16. All RIP routes will be assigned this weight.

The Corente Services Gateway implementation of RIPv2 complies with RFC 2453.

OSPF

Open Shortest Path First (OSPF) is a protocol that, like RIPv2, is used for routing IP traffic. It is a link-state protocol. A link can be considered an interface on the router, and the state of the link is a description of that interface and of its relationship to its neighboring routers. The collection of all these link-states forms a

link-state database. OSPF uses a link-state algorithm in order to build and calculate the shortest path to all known destinations.

The Corente Services Gateway will support OSPF multicast messages. The Corente Services Gateway can accept unicast messages from routers, but will multicast the responses.

To enable OSPF on a gateway, the OSPF section on the Section 11.9.2, “Network Tab” of the Location form must be completed as follows:

- **Enable OSPF on LAN:** When this option is selected, the Location gateway will use OSPF to announce routes on the LAN that can used to reach remote application network subnets.
  - **Route Cost:** To change the cost of routes advertised by OSPF on the gateway, enter a new value in this field. The default cost is 1.
  - **ASN Number:** The default ASN number is 0. If you would like, you can enter a new value in this field.

The Corente Services Gateway implementation of OSPF complies with RFC 2328.

BGP

Like RIP and OSPF, Border Gateway Protocol (BGP) is a protocol that is widely used for routing IP traffic. BGP is especially useful in very large private IP networks where routes to these different subnets are changing dynamically. In general, it is more secure than RIP or OSPF, as it reduces the risk of middle man attacks by requiring that you specifically identify routing neighbors of the Corente Services Gateway rather than relying on them to announce themselves.

- **Enable BGP on LAN:** When this option is selected, the Corente Services Gateway will use BGP to announce routes on the LAN that can used to reach remote application network subnets.
  - **AS Number:** Enter the AS number of the LAN on which this Location gateway is installed.
  - **Password:** Enter the password that the Corente Services Gateway will use when receiving BGP packets from its neighbors.
  - **Neighbors:** This Corente Services Gateway's current BGP routing neighbors are listed in this table. When you enable BGP, you must add at least one neighbor in this table. Click Add to add a new neighbor, Edit to edit an existing neighbor, or Delete to remove an existing neighbor.

On the screen that is displayed, enter the IP address of the BGP neighbor on the Corente Services Gateway's LAN, the AS number of the other network it routes to, and, if applicable, the password to be used by the Location when sending packets to this neighbor. When you are finished, click OK to store this neighbor. Note that you can enter duplicate neighbor IP addresses in this table if they have different AS Numbers.

Using RIP, OSPF, and BGP on your Corente Services Gateway

RIPv2, OSPF, and BGP can be used simultaneously on the same network, and can both be enabled on your Corente Services Gateway at the same time. They are enabled individually for each Corente Services Gateway.

If RIPv2 and OSPF are enabled, when a tunnel is successfully established to a remote gateway partner, the local gateway will send RIPv2 and OSPF packets to routers on its LAN interface only that announce the most appropriate routes to the tunnel. All computers on a subnet within the LAN will use the same route to access the tunnel and the appropriate subnet on the other side. When tunnels are brought down, the local gateway will send RIPv2 and OSPF packets to routers on its LAN announcing that the routes are no longer valid.

BGP differs from the other protocols in that, when a tunnel is successfully established to a remote Location partner, the local Corente Services Gateway will send BGP packets only to the routers on its LAN interface that are explicitly listed as neighbors, announcing the most appropriate routes to the tunnel. Like RIPv2 and OSPF, all computers on a subnet within the LAN that has a router with BGP enabled and which is also listed as a neighbor of the Corente Services Gateway will use the same route to access the tunnel and the appropriate subnet on the other side. When tunnels are brought down, the local Location gateway will send BGP packets to its neighbors announcing that the routes are no longer valid.

The Corente Services Gateway will use its LAN interface only to send and honor RIPv2, OSPF, and BGP messages from local routers. RIPv2, OSPF, and BGP will not be sent from or honored by the Corente Services Gateway's WAN interface, and will not be sent over or received from application network tunnels and the Internet.

Additionally, the Corente Services Gateway will only advertise routes that can be used to reach remote application network subnets. RIPv2, OSPF, and BGP will not be used to advertise routes from one local subnet to another local subnet. Normally, the Corente Services Gateway will not use RIPv2, OSPF, or BGP to advertise routes that can be used to reach Corente Clients, unless the client is using a private non world-routable IP address. For example, if the gateway connects to the application network from a LAN. The gateway will never advertise routes for a subnet if the reachable address of the Corente Services Gateway falls into that subnet.

Routes advertised from the Corente Services Gateway with RIPv2, OSPF, or BGP will override routes that you have entered on the Routes tab if the weight of the dynamic route is equal to or less than the weight of the static route. If the weight of the dynamic route is greater than the weight of the static route, the static route will be used first. A lower weight gives greater precedence to routes.

If you enable RIPv2, OSPF, and BGP, you do not need to add routes to the subnets on the Routes tab. However, you must have an entry on the User Groups tab for these subnets so that the machines on the subnets can participate in the application network. You must also make sure that there are routers on your local network that know about these subnets and you must configure these routers to respond to RIPv2, OSPF, or BGP messages.

Turning on RIPv2, OSPF, and BGP on your Network Routers

If you plan to use RIPv2, OSPF, and BGP to advertise routes on your multiple subnet LAN, you must turn on RIPv2, OSPF, and BGP on the appropriate network routers. For more information about turning on RIPv2, OSPF, and BGP, refer to the documentation provided with your router.

11.9.2.4 WAN Interface Mismatch

To prevent the possibility of intruders duplicating one of your Locations and gaining access to your domain, you can enable the Reject WAN Interface Mismatch security feature. If this feature is enabled for a Location and it attempts to connect with the Corente SCP when the IP address or MAC address of its WAN interface or WAN/LAN interface are not the same as the IP address or MAC address that were used the last time the Location was in contact with the Corente SCP, an alarm will be generated and the Location will be denied from contacting the Corente SCP. You should contact Oracle Support if this occurs.

If a WAN Interface mismatch occurs because you moved or swapped the hardware for the Location without selecting the Allow One WAN Interface change option described below, select that option and save your changes to the Location form. This Location will then be allowed to connect to the Corente SCP and function as usual.

Complete the fields as follows:

- **Reject WAN Interface Mismatch:** When this option is selected, if the Location contacts the Corente SCP and the IP address or MAC address of the WAN interface (or WAN/LAN interface) have changed, the Location will be denied from contacting the Corente SCP and an alarm will be generated.

When this option is selected, the following checkbox will be made available:

- **Allow One WAN Interface Change:** If you plan to move or change the hardware for the Corente Services Gateway, select this option first. This allows the new hardware to establish a secure connection with the Corente SCP with its new IP address and MAC address, which will be recorded at the Corente SCP. Once the new IP address and MAC address are recorded, this option will be deselected and the Reject WAN Interface Mismatch feature will function as described above. You must reselect this option the next time you would like to change the hardware.

11.9.2.5 Other Settings

The Other Settings section captures your preferences regarding nested subnets, remote access to Gateway Viewer, and the session re-key interval.

You can enable any of the following options:

- **Perform DNS/WINS Fixup:** If a computer has name services such as DNS or WINS configured on the system, the name used by the computer to make a connection will be resolved by DNS or WINS. For name resolution, the IP address of a computer that is stored on a DNS or WINS server is usually the computer's real IP address. If NAT occurs between two Corente Services Gateway partners within the application network, computers on one network of the application network will not be able to use the real IP address returned from DNS or WINS to connect to remote computers on the other network.

  The problem can be solved with DNS/WINS Fixup. If the Perform DNS/WINS Fixup option is checked, computers behind this Corente Services Gateway will always use the correct IP address to connect to another computer across the application network, either its real or NATed IP address. To provide this service, all packets from DNS/WINS servers within the application network are redirected to the DNS/WINS proxy on the Corente Services Gateway. Every name query response packet is checked and, if necessary, its contents are updated. The final DNS/WINS response packet with correct IP information is then forwarded to the original requester. The fixup is done automatically and is completely transparent to the end users. This feature allows all computers behind the Corente Services Gateway, including Corente Clients, to connect by name to remote NATed computers within the application network, using any application (such as ftp, http, telnet, and ping).

  Note

  The **DNS/WINS Fixup** will work only when name resolution requests are made via the Corente Services Gateway. This means that the DNS/WINS servers cannot reside on the same subnet as the computers using this service. Also, the fixup applies only to DNS/WINS packets within the application network. Therefore, a computer using DNS/WINS servers on the Internet will not benefit from this feature. Computers behind the Corente Services Gateway can have different DNS/WINS configurations as long as the Corente Services Gateway is in the name service request path.

  By default, this option is disabled.

- **Nested Subnets:** When you create a User Group for your Location during Location gateway creation in the Location Wizard, or on the User Groups tab, you indicate one or more ranges of IP addresses in your local network that will participate in the application network. Each Corente Services Gateway has one or more User Groups.

  By default, the service will not permit ambiguous handling of any IP address. For example, this means that no conflicting rules are permitted where the same IP address exists in a User Group for the local Corente Services Gateway and also exists in a User Group for this remote Location partner.

However, many network administrators make use of the fact that normal IP routing rules are ordered so that a more specific rule applies before a more general one. If there are conflicting rules for certain IP addresses, the rule describing the smaller subnet would take precedence. For example, a central site might have a User Group that includes all of 172.16.0.0/16 and a remote Location partner might have a User Group that includes 172.16.1.0/24. The remote Location partner's User Group description would override the central site's User Group because it contains a more specific range of addresses. Notice that the remote partner's User Group is completely contained inside the central site's User Group. This is what is referred to as a "nested subnet". Address ranges that overlap each other entirely are never permitted between Locations.

When this option is checked, nested subnets as described above will be permitted by this Corente Services Gateway. It is recommended that you do not check this option, as nested subnets can cause routing problems that are difficult to diagnose.

By default, this option will be unchecked for new Location gateways. When this option is unchecked, nested subnets will cause a Configuration Alert and no tunnels will be established between this Location and its partners.

A Configuration Alert for nested subnets can be prevented between two Locations that are partners, if you:

- Enter mutually exclusive IP address ranges in the User Groups
- Enable Allow Locations to be configured with nested subnets for both Locations
- Enable Auto Resolve NAT on both Corente Services Gateways for each other. Auto Resolve NAT is enabled by a Location on a per partner basis. If any conflicts occur between a Location and its partner when Auto Resolve NAT is enabled, the Corente Services Gateway will automatically translate the IP addresses of the partner's User Group to new subnets to prevent the conflicts.)

- **Compact NAT Subnets:** When this option is selected, the Location will sort addresses largest to smallest in order to keep the NAT table to a minimum. This feature applies to both Inbound NAT and Auto Resolve NAT. Locations have this option enabled by default.
- **Session Re-Key Interval:** Session keys are used by a Corente Services Gateway to encrypt the data that is being sent over each of its application network tunnels. A Corente Services Gateway will automatically regenerate its session keys according to the interval that you select with this pull-down menu. The default interval is 8 hours. You may choose a shorter interval,if you prefer.

11.9.2.6 LAN DHCP Server

When you click the **LAN DHCP Server** button on the **Add Interface** window, the **Edit LAN DHCP Server** window will be displayed.

Select the **Enable LAN DHCP Server** option and fill out this window as follows to configure how DHCP leases are served to computers on the Location's LAN:

- **DNS Suffix:** If you would like, enter a DNS suffix to be served to LAN computers by DHCP. When these computers submit a name for DNS name resolution, this DNS suffix will be appended to that name.
- **Serve DNS with DHCP:** This option enables you to select whether or not to pass the DNS Server IP addresses with the DHCP leases. When this box is selected, the computers on your LAN will be passed the DNS server addresses that are on the Section 11.9.2, “Network Tab” of this Location form.
- **Serve WINS with DHCP:** This option enables you to select whether or not to pass WINS Server IP addresses with the DHCP leases. WINS is the network protocol used in Windows networking; the

computer names you see in Network Neighborhood are all resolved into IP addresses, and vice versa, using WINS. When this box is checked, you must enter the IP addresses of the WINS server on your network. These are the addresses that will be passed.

- **Primary WINS:** Enter the IP address of the primary WINS server used to resolve WINS names on your local network.
- **Secondary WINS:** Enter the IP Address of the secondary WINS server that will be used to resolve names if the primary WINS server does not respond. You cannot enter a Secondary WINS address if you have not entered a Primary WINS entry.

- **Lease expires:** If this box is unchecked, the leases that the DHCP server assigns to local computers will be infinite. An address will not change unless the computer reboots. However, if this box is checked, the IP addresses will be temporary assignments. You must then specify in the fields that follow the number of days, hours, and minutes that the addresses should be used. When the specified amount of time is over, the lease is renewed. A lease is also renewed when a computer reboots. The renewed lease may or may not contain the same addresses.

Note

A DHCP Server saves you from the task of manually assigning IP addresses to computers on the Location's subnet. However, each user computer must be configured to obtain IP addresses automatically. In Windows, for example, this can be accomplished easily using the Network option in the Control Panel.

DHCP Address Ranges

When you select the Address Ranges tab in the lower half of the window, this section enables you to create the address pools that will be served by the Location.

Note

The ranges that you create here must correspond with address ranges that are included in the Default User Group on the User Groups tab of this Location’s Location form, to ensure that these computers can participate in the application network.

To begin creating address pools, select the **Add** button.

On this screen that is displayed, enter the following:

- **Include Address Range:** Select this option to indicate that the entire range you enter here will be served by DHCP.
- **Exclude Address Range:** After defining an Included range, you can exclude certain addresses from that address pool with this option. Enter the range of IP addresses that you would like to exclude from the included range in the Start Address and End Address fields. These addresses will not be served by DHCP. Note that the address of the Corente Services Gateway is automatically excluded and does not need to be entered here.

After selecting **Include** or **Exclude**, enter the following:

- **Start Address:** Enter the lowest value of the address range in this field.
- **End Address:** Enter the highest value of the address range in this field. If the range you would like to create contains only one IP address, you do not have to enter anything in this field.

Select the **OK** button to store this pool. Select **Cancel** to discard your changes and close the window.

DHCP Reservations

When you select the Reservations tab in the lower half of the window, you can reserve specific IP addresses for machines on the LAN that receive their addressing from the Location's DHCP server.

To begin reserving addresses, select the Add button.

- **Display Name:** Enter a name that will be used to identify this reservation on the App Net Manager interface.
- **IP Address:** Enter the IP address that will be reserved by the Location's DHCP server for use by this machine only. The machine will always receive this address from the DHCP server.
- **Reserved:** When this checkbox is selected, the IP address you entered will be saved and assigned to the machine whenever it receives its addressing via the Location's DHCP server.
- **MAC Address:** If this field is not already filled in, enter the MAC address of the machine for which the reservation is being made. This is how the DHCP server will identify the machine that will receive the reserved IP address.
- **NetBIOS Name:** If the Location has received information from the backend about the machine for which you are reserving an address, this field will display the Net BIOS name of the machine. This field will not accept manual input.

Select the **OK** button to store this reservation. Select Cancel to discard your changes and close the window.

The Location may receive MAC address information from the backend about clients on the LAN. In that case, those machines will be listed on the table on the right side of the App Net Manager interface when you open the Location in the domain directory, open the Network Interfaces entry, open LAN DHCP Server or RAS Client DHCP Server, and click DHCP Reservations.

Double click any entry in this table and the **Edit DHCP Reservation** dialog box will be displayed for that machine. Click the Reserved checkbox for this machine to ensure that the machine is served the IP address that you enter on this dialog box every time it receives addressing information from the gateway’s DHCP server.

DHCP Options

When you select the Options tab in the lower half of the window, you can include DHCP options that will be delivered along with addressing information by the Location's DHCP server. These options will be delivered to every device on the LAN that receives its addressing information via DHCP. The receiving device itself will determine whether or not it will use the option string. A typical use for option strings is for configuring handsets for IP telephony.

To begin reserving addresses, select the **Add** button.

- **Option Number:** Enter the option number that defines this option.
- **Option String:** Enter the string for this option. Only text string options are supported by Corente Cloud Services Exchange. Select the **OK** button to store this option. Select **Cancel** to discard your changes and close the window.

11.9.3 Applications Tab

The **Applications tab** enables you to register applications with this location, which can then be shared with any location in your Corente Services network and monitored via the Working with Reports feature of App Net Manager.

You can monitor not only the status and availability of the applications, but also usage, bandwidth, and latency/packet loss statistics per application and per application server.

Corente Cloud Services Exchange application monitoring is designed to be used as follows:

- To confirm to both users and administrators that applications are functioning correctly
- To facilitate communication between both parties when they are not
- To provide reports to help with capacity planning
- To provide diagnostic capabilities to locate bad actors within the network.

You can share and monitor any TCP-based application, as well as any of the following types of applications: Email (SMTP, IMAP, and POP), Web (HTTP and HTTPS), Authentication (LDAP), FTP, DNS, and Microsoft File Shares. If the applications you would like to register are not deployed on local servers, the Corente Services Gateway must be able to communicate with the servers either over the Internet or through alternate methods (such as via a private backbone or alternate connection).

The main screen of the Applications tab displays a table of all applications that you have already added.

You may **Edit** or **Delete** any application listed in the table.

11.9.3.1 Adding a New Application

Select the **Add** button on the main screen of the Applications tab. The **Add Application** screen will be displayed.

Complete the following fields and options:

- **Application:** Enter the name of the application as you would like it to appear to users and administrators.
- **Type:** Select the type of application that you are registering with the Location gateway. The following choices are available: Authentication Server, DNS Server, FTP Server, File Server, Generic Server, Mail Server, or Web Server. Select Generic Server when the application you are registering does not fit into the other categories.

  Your choice will affect the protocols that you may choose from when you add Application Policies.
- **Monitoring Enabled:** Select this option to enable monitoring of this application. If you do not select this option, this application can be shared with other locations, but will not be monitored via Reports or in Gateway Viewer.
- **Participates in Secure Network:** Select this option to allow this application to be shared over your Corente Services application network. If this option is not selected, you will not be able to share this application like a User Group with other locations. Note that on the Monitoring interface in Gateway Viewer, the application will be listed in the Service Availability Summary section to designate this application as a locally-used application and to differentiate this application from those being shared over the application network, which are listed in the Application Status Summary section.
- **Notification on Failure:** Email: Select this option if you would like the application's administrator to receive an email notification if this application should fail. The notification will be sent to the email address supplied in the Owner Email field. If no email address has been entered that field, the notification will instead be sent to the addresses supplied on the Alerts tab for this Location. .
  - **Owner Email:** Enter the email address of the administrator of this application. All email notifications will be sent to this address. Additionally, this email address will be published to any user in Gateway

Viewer that has the appropriate permissions to use this application, so that they can communicate directly with the appropriate administrator, if necessary.

- **Notification on Failure:** SNMP: Select this option if you would like to receive an SNMP trap if this application should fail. The SNMP trap will be sent according to the SNMP version and parameters that you specify on the SNMP tab of this Location form.
- **Host Server Name:** Enter the DNS name of the server providing this application.
- **Host Server IP:** Enter the IP address of the server providing this application.

Note

The following network addresses are restricted and cannot be assigned to any hosts on the LAN:

- 1.1.1.0
- 1.1.1.1
- 1.1.1.2
- 1.1.1.3

- **QoS Settings Inbound:** If you would like, choose a QoS entry from the pulldown menu to specify the priority of traffic inbound through the Corente Services Gateway to this application. QoS entry definitions in this menu can be viewed or modified with the Section 10.3, “Quality of Service (QoS)” feature.
- **QoS Settings Outbound:** If you would like, choose a QoS entry from the pulldown menu to specify the priority of traffic outbound through the Corente Services Gateway from this application. QoS entry definitions in this menu can be viewed or modified with the Section 10.3, “Quality of Service (QoS)” feature.

Note

As when performing any sort of QoS configuration, administrators must be careful when assigning QoS levels because if there is too much high priority traffic, any other traffic with a lower level of priority may become too slow or even be dropped. In addition, you cannot use QoS to prioritize traffic to or from a Corente Client.

After providing basic information about the application, you must use the **Modify Application Policies** section to register the policies of this application. A policy is essentially a combination of protocol and port number that the application's server uses to communicate with the machines that connect with it, or that the machines use to communicate with the server.

The **Application Policies** table lists all the policies that you have already added. You may **Edit** or **Delete** any policy listed in the table. Click **Add** to create a new policy.

On the screen that is displayed, enter the following:

- **Protocol:** Select the protocol for this policy. The protocols that are available depend on to the Application Type that was chosen for this application.
- **Port:** Enter the port number for this policy.
- **Direction:** Select the direction of the traffic that you are regulating with this policy. For example, traffic that travels in through the Corente Services Gateway to the server, out through the Location gateway from the server, or both.

- **Administered Application Policy Tests:** Application policy tests are tests that are used by the Corente Services Gateway to monitor the application and determine if it is functioning correctly or not. Depending on the test chosen, you will choose thresholds that cause a Warning alarm and a Critical alarm. The types of tests that are available depend on the protocol that you chose for this Application Policy. Each test that you enable will be performed on the application's traffic once a minute.

  The table lists all the tests that you have already added. You may Edit or Delete any test listed in the table. Click Add to create a new test.

On the screen that is displayed, enter the following:

- **Application Policy Test Name:** Select the test you would like to enable from the pull-down menu.
- **Application Policy Test Arguments:** When an Application Policy Test Name is selected, this table lists all of the arguments for that test. To modify the variable for an argument, select the argument and click the blue text in the Variable column. You can enter a new value in the field that is provided.

  All Application Types allow you to create policies for ICMP, TCP, and UDP protocols. The following table describes the Policy Tests that you may choose for each of these protocols and what they monitor:

Table 11.1 Policy Tests for ICMP, TCP, and UDP Protocols

Protocol	Test Types	What Test Monitors
ICMP	ICMP PING	This is a standard test that checks the application server for availability. Warning and critical alarms are based on the latency and loss of test packets.
	Roundtrip Latency	This test monitors the average round trip latency of packets sent to and from the applications server.
	IP Network Quality	This test estimates network quality by measuring a combination of latency, jitter, and packet loss on traffic samples in an interval. The administrator sets acceptable thresholds for latency (in milliseconds) and loss (in percent of packets in the interval). In addition, the length of the jitter buffer (in milliseconds) is also set as the jitter threshold. Each traffic sample is evaluated as acceptable or defective in the following manner: • If jitter in the sample surpasses the specified jitter threshold, it is treated as a lost packet. If it does not surpass the jitter threshold, the jitter is treated as latency.

Protocol	Test Types	What Test Monitors
		• The latency in excess of the latency threshold and the packet loss in excess of the packet loss threshold are then plugged into an equation that more heavily weights loss against latency. • The results of the equation are then compared to an acceptability threshold that is set by the administrator to determine whether the traffic sample is acceptable or defective. Administrators can specify or use defaults for: Warning and Critical alarm thresholds based on percentage of defective samples in an interval. Interval in seconds over which the percentage of defective samples will be computed. Acceptability threshold (excess packet loss squared times four plus excess latency). Latency threshold. Jitter threshold. Loss threshold.
TCP	ICMP PING	See ICMP PING above.
	Roundtrip Latency	See Roundtrip Telephony above.
	IP Network Quality	See IP Network Quality above.
	TCP Connection	This test monitors the TCP connection of the application.
UDP	ICMP PING	See ICMP PING above.
	Roundtrip Latency	See Roundtrip Telephony above.
	IP Network Quality	See IP Network Quality above.
	UDP Connection	Like the TCP Connection test, but for the UDP protocol.

In addition to the protocols above, some of the Application Types allow you to create policies for application-specific protocols. In addition to the ICMP PING, Roundtrip Latency, IP Network Quality, and occasionally the TCP Connection test, these protocols each have a protocol-specific test:

Table 11.2 Policy Tests for Application-Specific Protocols

Application Type	Protocol	Test Types	What Test Monitors
Authentication Server	LDAP	LDAP Lookup	This test monitors the response time for LDAP packets sent to the LDAP server.

Application Type	Protocol	Test Types	What Test Monitors
DNS Server	DNS	DNS Lookup	This test monitors accuracy of the DNS server: you supply a DNS hostname and the IP address that should be returned by the server. In addition, the test monitors the response time and raises a **critical** alarm when the request has timed out.
FTP	FTP	FTP Handshake	This test monitors the response time for FTP packets sent to the FTP server.
File Server	NETBIOS	File Share	This test measures disk usage percentage. You must supply a share name, username, and password to allow the Corente Services Gateway to log onto the File server.
Mail Server	IMAP	IMAP Handshake	This test monitors the response time for IMAP packets sent to the IMAP server.
	POP	POP Handshake	This test monitors the response time for POP packets sent to the POP server.
	SMTP	SMTP Handshake	This test monitors the response time for SMTP packets sent to the SMTP server.
	Secure IMAP	Secure IMAP Handshake	This test monitors the response time for Secure IMAP packets sent to the IMAP server.
	Secure POP	Secure POP Handshake	This test monitors the response time for Secure POP packets sent to the POP server.
Web Server	HTTP	HTTP Transaction	This test monitors the response time of HTTP packets sent to the HTTP server by accessing a specified web page. When an

Application Type	Protocol	Test Types	What Test Monitors
			optional Expected Status (string to expect in the first status line of server response) is specified, this test can be used to look for specific HTTP error codes, such as 400. If the string is not found, a CRITICAL alarm is raised. When an optional Expected Expression is specified, the test will search the page returned by the web server for a case-insensitive regular expression. If the specified pattern is not found, a CRITICAL alarm is raised. When an optional Redirection Handling option is specified and the test results in a redirect to another webpage, you can choose to generate no alarm, a WARNING alarm, a CRITICAL alarm, or the redirection can be followed.
	HTTPS	Secure HTTP Transaction	Similar to the HTTP Transaction test, but for HTTPS.

When you have finished configuring an Application Policy Test, click **OK** to store your changes or Cancel to close the window and discard your changes. You may add as many tests to an Application Policy as you would like.

When you have finished configuring an Application Policy, click **OK** to store your changes or Cancel to close the window and discard your changes. You may add as many Application Policies to a monitored application as is required by that application.

When you have finished configuring an Application, click **OK** to store your changes or **Cancel** to close the window and discard your changes. The application will be added to the main screen of the **Applications** tab.

On the Section 11.9.7, “Partners Tab”, you can define permissions by including the applications that you register on this screen in tubes. Tubes allow you to specify a set of remote machines and remote applications that are allowed to communicate with your locally-defined applications, so that you can share these applications with specific computers in any other Location.

11.9.4 Monitored Servers Tab

The **Monitored Servers** tab enables you to register servers with this Corente Services Gateway in order to monitor the availability of these servers and the usage of certain resources on these servers, such as CPU, physical memory, disk space, and swap space. You can define thresholds and will be alerted when usage exceeds these thresholds. In addition, all monitored data can be viewed in Gateway Viewer and with the Reports feature.

11.9.4.1 Requirements for Using SNMP

A Corente Services Gateway uses the Simple Network Management Protocol (SNMP) to monitor servers. Any servers to be monitored must have an SNMP agent installed on them. For Windows servers, the SNMP Windows component is required. For all other operating systems, is is best to use the NET-SNMP agent. But you can use any other agent, as long as it supports the Host Resources MIB as defined in RFC 2790.

You can monitor any server that meets the following requirements:

- The monitored server must support SNMP Version 1 (as defined in RFC 1157) and be able to respond to polls from SNMP network management stations.
- The monitored server must support the Host Resources MIB (as defined in RFC 2790).
- If the monitored server is not on the same LAN as this Corente Services Gateway, the Corente Services Gateway must be able to communicate with the server either over the Internet or through alternate methods (such as via a private backbone or alternate connection).

11.9.4.2 Configure SNMP

To monitor a Windows server, you must be logged in as an administrator or a member of the Administrators group. Click **Start** and go to the **Control Panel**, double-click **Programs and Features**, then click **Turn Windows features on or off** in the left-hand side of the page.

Select the **Simple Network Management Protocol** check box, and click **OK**, then click **Next**.

You may be required to insert the Windows Operating System CD when installing this component.

To configure the SNMP agent, access the Control Panel. Double-click **Administrative Tools** and then double-click **Computer Management**.

In the console tree, click **Services and Applications** and then click **Services**.

In the details pane, scroll down and click **SNMP Service**.

From the **Action** menu, click **Properties**.

On the **Security tab**, select **Send authentication trap** if you want a trap message to be sent whenever authentication fails.

Under **Accepted community names**, click **Add**.

Under **Community Rights**, select a permission level for this host to process SNMP requests from the selected community.

In **Community Name**, type a case-sensitive community name, and then click **Add**.

Specify whether or not to accept SNMP packets from a host:

- To accept SNMP requests from any host on the network, regardless of identity, click **Accept SNMP packets from any host**.

- To limit acceptance of SNMP packets, click **Accept SNMP packets from these hosts**, click **Add**, type the appropriate host name and IP or IPX address, and then click **Add** again.

Click **Apply** to apply the changes.

Register the server in the Location form of the local Location gateway.

11.9.4.3 Configure Server Monitoring

The main screen of the **Monitored Servers tab** in the Location form presents a table of all servers that you have already added to be monitored. You may **Edit** or **Delete** any server listed in the table.

To add a new server to the table, follow the instructions in Section 11.9.4.4, “Add a New Server for Monitoring”.

11.9.4.4 Add a New Server for Monitoring

Select the **Add** button on the main screen of the Monitored Servers tab. The **Add Monitored Server** window will be displayed.

Fill out the fields and options as follows:

- **Name:** Enter the name of the server as you would like it to appear to administrators in Gateway Viewer.
- **Notify via Email on Failure:** Select this option if you would like the server's administrator to receive an email notification if this server reaches its warning or critical thresholds, or if it should fail. The notification will be sent to the email address supplied in the **Server Owner Email** field. If no email address has been entered that field, the notification will instead be sent to the addresses supplied on the Alerts tab for this Location.
- **Server Owner Email:** Enter the email address of the administrator of this server. If you have selected the **Notify via Email on Failure** option, all email notifications will be sent to this address.
- **Type:** Select the type of server that you are registering with the Location gateway. The following choices are available: Default (MIB II Host), FreeBSD NET-SNMP, LINUX Net-SNMP, NET-SNMP OS Independent, Solaris NET-SNMP, Windows Server 2008, Windows Server 2012, Windows 10, and Windows Server 2016.

Note

If your server uses an operating system other than Windows and is using an SNMP agent other than the NET-SNMP agent, you must choose the Default (MIB II Host) server type. Make sure that the SNMP agent you are using on the server supports the Host Resources MIB (aka MIB II Host) as defined in RFC 2790.

- **Host Name:** Enter the DNS name of the server.
- **Host IP:** Enter the IP address of the server.

After providing basic information about the server, you must use the Monitored Server Tests section to register the tests of this application. Server tests are tests that will be performed on the server to identify usage statistics for different resources: CPU load, disk space, memory usage, and swap space. This table lists all the tests that you have already added. You may **Edit** or **Delete** any test listed in the table. Click **Add** to add a new server test.

On the screen that is displayed, enter the following:

- **Monitored Server Test Name:** Choose from four resources that can be monitored: CPU Usage, Disk Usage, Memory Usage, and Swap Usage.

- **Monitored Server Test Arguments:** When a Monitored Server Test Name is selected, this table lists all of the arguments for that test. To modify the variable for an argument, select the argument and click the blue text in the Variable column. You can enter a new value in the field that is provided.
- When you have finished defining a server test, click **OK** to store your changes or **Cancel** to close the screen and discard your changes. You can enable as many of the tests for a server as you would like. When you have finished defining a monitored server, click **OK** to store your changes or **Cancel** to close the screen and discard your changes. Your new monitored server will now appear on the main screen of the Monitored Servers tab.

11.9.5 User Groups Tab

The User Groups tab lets you identify groups of machines on the local network, such as computers, servers, and printers, that are allowed to participate in your application network.

11.9.5.1 Introduction to User Groups

- To begin, you must edit the Default User Group, which provides the Corente Services Gateway with a list of all machines on the LAN that are participating in the application network. You first created this group when you used the Location Wizard to create the Location.
- Next, if applicable, you should define your Default User Group – DMZ, which informs the Corente Services Gateway what subnet is designated as the DMZ on your LAN.
- Then, you should define the Internal Network Description group, which should contain all of the subnets at your site. This allows the Corente Services Gateway to distinguish between computers on the Internet and computers on the LAN that are not participating in the application network.
- After you define these User Groups, you can create additional named User Groups, which will divide the IP addresses on the LAN into smaller groups. Each named User Group consists of machines that will have the same permissions on the domain or LAN. You can create any number of named User Groups for this Location.

On the Section 11.9.7, “Partners Tab” or with the Tube wizard, you can further define and restrict permissions by including your User Groups in tubes. Tubes enable you to specify a set of local machines, a set of remote machines or a remote application, and the firewall policy to be used when these machines communicate.

Important

The following network addresses are restricted and cannot be assigned to any hosts on the LAN:

- 1.1.1.0
- 1.1.1.1
- 1.1.1.2
- 1.1.1.3

Instead of using the User Groups tab to include application servers on the LAN in your application network, you may want to register these servers on the Section 11.9.3, “Applications Tab”.

The main screen of the User Groups tab displays the User Groups that have already been configured for this Location. Three placeholder User Groups appear by default:

- **Entire LAN Group:** This group is used on the Partners tab exclusively when creating a LAN to Internet Access or LAN to Location Access partnership. It is predefined and cannot be modified.
- **Location LAN Address:** This group is used on the Partners tab when creating a LAN to Location Access partnership or a partnership that allows partners to access the Gateway Viewer application for this Location. It is predefined and cannot be modified.
- **Default User Group:** This group contains every IP address on the LAN that will participate in the application network. It is not predefined and must be configured before a new Location gateway can be installed.
- **Default User Group - DMZ:** (appears only when a DMZ interface has been configured for this Location on the Network tab) This group contains every IP address on the LAN that is participating in the DMZ. Depending on the choices you made when configuring the DMZ interface, this group may or may not be predefined. This group is used exclusively when configuring the DMZ to Internet Access and LAN to DMZ Access partnerships on the Partners tab.

11.9.5.2 Create the Default User Group

Each Location must have a Default User Group. The Default User Group must contain every IP address on the LAN that will participate in the application network. You created a Default User Group in the Location Wizard when you created your Corente Services Gateway personality, but you can modify this group using the following procedure. To configure the Default User Group, select the Default User Group entry on the main screen of the User Groups tab and select the Edit button. The Edit User Group 'Default User Group' screen will be displayed

On this screen, you must define which computers on the local network will participate in the application network by specifying subnets of IP addresses.

- **Firewall Policy:** If you would like, you can choose an optional Firewall Policy that will apply to all traffic to and from the Default User Group.
- **Inbound QoS:** If you would like, you can choose optional Quality of Service (QoS) settings for traffic inbound to the default User Group. To specify the priority of traffic inbound through the Corente Services Gateway to the default User Group, choose a QoS entry from the Inbound QoS pulldown menu.
- **Outbound QoS:** If you would like, you can choose optional QoS settings for traffic outbound from the default User Group. To specify the priority of traffic outbound through the Location gateway from this User Group, choose a QoS entry from the Outbound QoS pulldown menu.

Note

As when performing any sort of QoS configuration, administrators must be careful when assigning QoS levels because if there is too much high priority traffic, any other traffic with a lower level of priority may become too slow or even be dropped. In addition, you cannot use QoS to prioritize traffic to or from a Corente Client.

- **User Group is Within Secure Network:** This option will be chosen by default and cannot be changed.
- **Special Internal Network Description Group:** This option will not be chosen by default and cannot be changed.
- **User Group Subnet/Address Ranges:** This section enables you to define the subnets/ranges that you would like to include in the Default User Group. The table lists all the ranges that you have already added. You may Edit or Delete any range listed in the table.

  To add a new subnet/range, select the Add button.

- **Include Subnet:** Select this option to specify a range that will be included in the group. Fill out the available fields as follows:
  - **Network Address:** Enter the first address of the subnet in this field.
  - **Subnet Mask:** Enter the net mask of the subnet in this field, which will define the range of addresses within this subnet.

> **Note**
>
> If you include a range of IP addresses that is not contained within the same subnet of the LAN IP Address of the Corente Services Gateway or not distributed by the Corente Services Gateway's DHCP server, you must either provide routing information to this subnet on the Section 11.9.6, "Routes Tab" of this form or enable RIPv2 or OSPF on the Section 11.9.2, "Network Tab" of this form.

- **Outbound NAT:** You must set the appropriate Outbound NAT settings for this subnet. Network Address Translation (NAT) is used to map the real IP address of each machine in a subnet to an IP address within another subnet. The translated IP addresses become the visible IP addresses of the machines. NAT can be used to organize a network or prevent routing problems caused by duplicate IP addresses.

  When Outbound NAT is enabled for a Location, the Location gateway will translate the subnet of IP addresses to another subnet before the Corente Services Gateway makes the addresses visible to remote partners. The administrator must specify the new subnet to which the real IP addresses will be translated. Each address within the real subnet will be mapped to an address in the specified subnet. For all remote partners, these specified addresses will become the visible IP addresses of the machines.

- **The Outbound NAT** settings in your User Group will interact with the Auto Resolve NAT and Inbound NAT settings that a Location partner has chosen for your Location.
  - **Prohibited:** This setting forbids all partners to perform NAT on this Location's User Group. If Prohibited has been set on a range in the local User Group and a partner has enabled Auto Resolve NAT (and there is an address conflict) or Inbound NAT for this Location, the tunnel will not be brought up and a Configuration Alert will be generated. In other words, the Prohibited setting will bring down any tunnel to a partner if that partner attempts to NAT this User Group. The primary use for this setting is to prevent NATing on a connection that is transporting a protocol containing embedded IP addresses for which the Corente Services Gateway does not have a fixup module. The Corente Services Gateway includes a fixup module that allows active FTP, normally forbidden on a NATed subnet.
  - **Permitted:** This is a passive setting. The Corente Services Gateway will not NAT the address range, but it will not prevent the address range from being NATed by a partner. This is the default setting.
  - **Specified:** This setting allows an administrator to specify a new subnet of IP addresses to which this address range will be mapped. The new addresses within the specified subnet will become the visible IP addresses of the local computers in this range to all remote partners. After enabling this option, enter the new subnet in the Specified NAT Address field. This address space must be unique in the application network.

    The Specified setting is a useful way of organizing an entire domain, where each User Group in the domain is mapped to a distinct set of address ranges so that there are no address conflicts. The traffic from each site can then be identified by the range into which it has been mapped. Of course, it is the administrator's responsibility to guarantee that there are no conflicts between the addresses that have been Specified for each subnet. Therefore, it is usually preferable to specify Inbound NAT for conflicting addresses (configurable on the Partners tab) rather than use Outbound NAT, because

Inbound NAT does not require a global solution and there are no chances for conflicting addresses after the solution has been applied.

- **Exclude Range:** If there are IP addresses or ranges of addresses within the subnets that you have already Included that you do not want to be in your Default User Group, you can use the Exclude Range option to remove these addresses. Select this option to specify a range that will be excluded in the group. Fill out the available fields as follows:

  - **Start Address:** Enter the first address of the range that you would like to be excluded from an existing included range.

  - **End Address:** Enter the last address of the range that you would like to be excluded from an existing included range. If the range includes only one address, you do not need to fill in this field.

  Click OK to add this definition to your Default User Group or Cancel to close the window and discard your changes. Repeat this process for as many subnets as you would like to add to your Default User Group. Remember that you must have at least one IP address listed as an include in the Default User Group even if you are using DHCP. In other words, DHCP is selected for a network interface on the Network tab of this form.

  When you are finished defining your Default User Group, click the OK button to store your changes and return to the main User Groups tab.

11.9.5.3 Create the Internal Network Description Group

After defining the Default User Group, you should map out the entire local corporate network, even those computers that are not participating in the application network. You will transfer this information onto your Corente Services Gateway on the User Groups tab, using the Special Internal Network Description User Group option. To configure the Internal Network Description User Group, click the Add button. The Add User Group screen is displayed.

Fill out the screen as described above in the Default User Group section. (Note that you will not be able to select NAT settings for Included subnets.) You must add all subnets within your LAN to this User Group, because this definition includes the entire network, even machines that are not participating in the application network. Select the Special Internal Network Description User Group option and make sure the User Group is Within Secure Network option is not selected.

When you are finished, click the OK button to save your changes and return to the main User Group screen. The Internal Network Description User Group will now be displayed on this screen.

This User Group allows the Corente Services Gateway to distinguish between the corporate network and the Internet, which is especially important when this Corente Services Gateway is acting as a Backhaul Server. It prevents traffic being sent from or received by computers on the LAN that are excluded from the application network for security reasons. For example, if an Internal Network Description User Group is not defined, a Location designated as a Backhaul Server might route non-application-network traffic from a Backhaul Client to one of its own non-participating subnets, believing the subnet's address to be part of the Internet.

11.9.5.4 Create Named User Groups

After defining the Default User Group, look at your LAN and decide what groups of IP addresses will need similar permissions in your domain and in any of your extranets. This means deciding what remote computers and applications each local computer will need to access or be accessed by, and what protocols must be allowed or denied over their secure connections. Divide your LAN's IP addresses and subnets into groups based on these criteria.

On the User Groups tab, you must configure these groups into named User Groups. You can define as many named User Groups as you need. Named User Groups in a Location can overlap with each other. However, you cannot create two named User Groups that contain the exact same set of IP addresses.

To configure a named User Group, click the Add button. The Add User Group screen will be displayed.

Complete the screen as follows:

- **User Group Name:** Enter a name for this User Group.
- **Firewall Policy:** If you would like, you can choose an optional Firewall Policy that will apply to all traffic to and from this User Group.
- **Inbound QoS:** If you would like, you can choose optional QoS settings for traffic inbound to this User Group. To specify the priority of traffic inbound through the Corente Services Gateway to this User Group, choose a QoS entry from the Inbound QoS pulldown menu.
- **Outbound QoS:** If you would like, you can choose optional QoS settings for traffic outbound from this User Group. To specify the priority of traffic outbound through the Corente Services Gateway from this User Group, choose a QoS entry from the Outbound QoS pulldown menu.

Note

As when performing any sort of QoS configuration, administrators must be careful when assigning QoS levels because if there is too much high priority traffic, any other traffic with a lower level of priority may become too slow or even be dropped. In addition, you cannot use QoS to prioritize traffic to or from a Corente Client.

- **User Group is Within Secure Network:** Select this option if you would like this User Group to participate in the secure network. This option is selected by default. There are occasionally reasons to create User Groups that are not within the secure application network. Remember that named User Groups within the application network must be subsets of the Default User Group (in other words, they can only include addresses that are also included in the Default User Group).
- **Special Internal Network Description Group:** This option will not be chosen by default and cannot be changed.
- **User Group Subnet/Address Ranges:** This section enables you to define the subnets/ranges that you would like to include in this User Group. The table lists all the ranges that you have already added. You may Edit or Delete any range listed in the table. To add a new subnet/range, select the Add button.

Note

When capturing the IP addresses to be included in a User Group, the Include Subnet and Exclude Range options cause the definition of the User Group to differ, as follows:

- When all groups of IP addresses in the User Group are specified as Included, the User Group will contain only those IP addresses listed.
- When all groups of IP addresses in the User Group are specified as Excluded, the User Group will contain all IP addresses within the Default User Group except for the excluded IP addresses.
- When some groups of IP addresses are specified as Included and some as Excluded, the User Group will contain only those IP addresses listed as Includes except for the excluded IP addresses.

- **Include Subnet:** Select this option to specify a range that will be included in the group. Fill out the available fields as follows:
  - **Network Address:** Enter the first address of the subnet in this field.
  - **Subnet Mask:** Enter the net mask of the subnet in this field, which will define the range of addresses within this subnet.

> **Note**
>
> If you include a range of IP addresses that is not contained within the same subnet of the LAN IP Address of the Corente Services Gateway or not distributed by the Corente Services Gateway's DHCP server, you must provide routing information to this subnet on the Routes tab or enable RIPv2 or OSPF on the Network tab of this form.

- **Exclude Range:** Select this option to specify a range that will be excluded in the group. Fill out the available fields as follows:
  - **Start Address:** Enter the first address of the range that you would like to be excluded from an existing included range.
  - **End Address:** Enter the last address of the range that you would like to be excluded from an existing included range. If the range includes only one address, you do not need to fill in this field.

  Click OK to add this definition to your User Group or Cancel to close the window and discard your changes. Repeat this process for as many subnets as you would like to add to your User Group.

When you are finished defining your User Group, click the OK button to save your changes and return to the main User Groups tab. The named User Group will now be displayed in the table.

11.9.5.5 Other User Groups

There are certain circumstances in which you may want to deselect the User Group is in Secure Network option when creating a User Group.

User Groups that are configured without the User Group is in Secure Network option selected can contain both machines that are participating in the application network and those that are not.

Using the Corente Services Gateway for Local Routing

In addition to serving as an application network router, a Corente Services Gateway also serves as a local router. To use this Corente Services Gateway to route local traffic to and from a subnet, add the subnet to a User Group on the User Groups tab. If the User Group contains any machines that are not participating in the application network, make sure the User Group is in Secure Network option is not selected for the User Group. Then, configure static routes between the Corente Services Gateway and subnets in the User Group on the Routes tab of this form or enable RIPv2/OSPF on the Network tab and the subnet routers.

The Corente Services Gateway will route traffic between this User Group and any other local subnets that are also included as User Groups.

11.9.6 Routes Tab

If your local network is organized into different subnets of computers and you would like more than one of these subnets to be included in your Corente application network, you can add static routes from your Corente Services Gateway to these computers with the Routes tab of the Location form.

Note

The computers on the subnets that you include on this screen will not be able to access the Gateway Viewer application unless you configure the routers on those subnets to forward UDP broadcast packets to the Corente Services Gateway.

The main screen of the Routes tab presents a table of all routes that you have already added. You may **Edit** or **Delete** any route listed in the table.

Adding a New Route

To combine different subnets, you must supply the IP address information for the machines that have access to both subnets. These subnet connections may exist through a computer with two Ethernet interfaces, known as a gateway, or through a networking device, known as a router. Both of these machines connect subnets into the same local network by having an IP address in each subnet.

Select the **Add** button on the main screen of the Routes tab. The Add Route screen will be displayed.

Fill out the fields and options as follows:

- **Network Address:** Enter the IP Address of the subnet to which you want to route.
- **Network Mask:** Enter the network mask of the subnet to which you want to route.
- **Gateway/Router IP Address:** Enter the IP address of the machine on your network that routes to the subnet to which you want the Corente Services Gateway to route. This address must be on the SAME subnet as your Corente Services Gateway.

Once you have filled in all of these fields, clicking on the OK button will add this information to the Routes tab.

Dynamic Routing via RIPv2, OSPF, or BGP

You can skip the process of entering route information on this screen if you decide to enable RIPv2, OSPF, or BGP on your local network. When enabled, the Corente Services Gateway will use RIPv2, OSPF, and BGP messages to determine the most appropriate routes for local subnets to use to reach the application network tunnel. The Corente Services Gateway will then advertise the routes to local network routers.

By default, dynamic routes broadcast with RIPv2, OSPF, and BGP will be used before static routes entered on the Routes tab.

Use the Corente Services Gateway for Local Routing

In addition to serving as an application network router, a Corente Services Gateway serves as a local router, as well. It will automatically provide routes between subnets that are both participating in the application network.

11.9.7 Partners Tab

Secure connections for your site-to-site traffic are provided by secure tunnels across the Internet between two Locations, or a Location and a Corente Client or mobile device. Each pair of Locations (or Location/client) is referred to as a set of partners. Each Location can have multiple partners. To enable partners for a Location and define the parameters of the partnership, you can do the following:

- Launch the Partners Wizard.
- Access the Section 11.9.7, “Partners Tab” for a Location.

- Create a drag and drop tunnel.

To choose Location partners and establish secure tunnel connections in your application network, access the Partner tab of the Location form for each of your gateways.

Using the Partners tab enables you to enable advanced functionality that is not available when using the Partner Locations wizard, but you must remember to configure the Partners tab for each Location involved in the partnership. Location partnerships are reciprocal and must be defined on both sides of the partnership.

The Partners tab can also be used to configure an optional Internet firewall for your LAN and to limit which local and remote computers will have access to this Corente Services Gateway to perform such functions as monitoring it with SNMP or connecting to its Gateway Viewer application.

Use the following procedure to create tunnel connections using the Partners tab of the Location form.

1. Access the Location form for a gateway:
   - Right-click the Location icon in the map or domain directory and select **Edit**.
   - Double-click the Location name in the domain directory.
   - Select the Location name in the domain directory and then select the **Edit** option from the toolbar or the Edit menu.

     The Location form will be displayed in a new window.
2. On the Location form, click the **Partners tab**. This tab is used to select the Locations, both Intranet and Extranet, and Corente Clients that will partner with this Location.
3. The main Partners tab presents a table of all partners that you have already added as well as four default partners: LAN to Internet Access, LAN to Location Access, DMZ to Internet Access, and LAN to DMZ Access. You may Edit or Delete any partner listed in the table.

   This table also displays the following basic information about each partner:
   - **Name:** The name of the partner.
   - **Type:** The type of partner (Regular, Access, Extranet, or Client Group).
   - **Status:** The current status of the tunnel between this Location and the partner.
   - **NAT:** The NAT setting for the tunnel between this Location and the partner.
   - **Conn Share:** Whether or not Connection Sharing is enabled for this partnership.
   - **Tubes:** The number of tubes that are defined for this tunnel.
   - **Transport:** The protocol encapsulating the packets that travel between these partners over the secure tunnel (UDP or TCP). This is determined automatically by the Corente Services Gateway. UDP is the preferred protocol, as it performs better under conditions where there is packet loss, but TCP will be used in cases when UDP cannot.
4. Select the **Add** button on the main Partners tab. The Add Partner screen is displayed.
5. Begin by filling out the Connection to Partner section. This section enables you to choose a partner for this Location. To begin, you must choose one of the following types of partners:
   - **Intranet:** Locations that are within this Location's own domain.

- **Extranet:** Locations from another domain that have been imported into this domain with the Extranet Imports and Exports feature, available in the domain directory, and have been permitted to contact this Location.
- **Client Groups:** Groups of Corente Clients that were created with the Client Groups feature and have been permitted to access this Location.
- **Mobile User Groups:** Groups of mobile users that were created with the Mobile User Groups feature and have been permitted to access this Location.
- **Third-Party Devices:** Devices, such as a Cisco router, which have been created with the 3rd-Party Devices feature.

  A third-party device which is configured as a backhaul server must be be the **only** partner for a Corente Services Gateway.

After selecting the type of partner you want to connect with this Location, select a Location (or a client group or third-party device) from the adjoining pull-down menu. If the Location has already enabled a connection to this Location on its Partners tab, the Connection Enabled by Partner checkbox will be checked. Note that connections to client groups are defined on the Location side of the partnership only, so this checkbox will always be checked when adding a client group as a partner.

6. Configure the settings on the Add Partner screen as appropriate and then enable at least one Tube on this partner connection.
7. When you are finished with the **Partners** tab, click **OK** to close the window. After you **Save** your changes, remember to access the **Partners** tab for the other Location partner and complete this process again. All Location partnerships are reciprocal.

11.9.7.1 Connection Settings

The **Connection Settings** section contains the following fields:

- **Use Connection Sharing (Port NAT):** Checking this box will cause all computers on the internal network to use the Location gateway's IP address and some unused port of the Corente Services Gateway's external interface as the source address and port numbers for any traffic destined for the selected partner. For Inline Locations, the WAN IP address of the Corente Services Gateway will be used for the LAN to Internet Access partner, and the LAN address will be used for the all other partners.

  When packets return to the Corente Services Gateway from the partner, the destination address and port are converted back to the original source address and port number pair. The Corente Services Gateway will handle the WAN IP address to internal IP address conversions automatically.

  This option is especially useful for Extranet connections, when you would like to hide your internal network from an untrusted partner.

- **Partner for Failover Only:** Select this option to use the selected partner as a Backup connection to a site if the connection to the Primary partner at that same site should fail. This option allows hub sites with multiple Corente Services Gateways to use load balancing to manage application network traffic by allowing multiple Corente Services Gateways to support the same User Group and applications.

- **Specify Failover settings for this connection:**. Failover is configured on the Section 11.9.10, "High Availability Tab" of this form.

  You can select this option to override the settings that you enter on the High Availability tab and define the failover behavior for the selected partner's connection to this Location only. For example, you may

want to override the High Availability tab settings and make the Failover/Failback detection interval (in seconds) longer on this screen if this partner uses a slower Internet connection or DSL, where short connection outages are common. When this option is selected, the following fields will be enabled and the default entries can be modified:

- **Failover/Failback detection interval:** The period of time that the partner will wait until it fails over to a Backup Location gateway after it detects that the connection to this Corente Services Gateway is down, and the period of time that the partner will wait after it detects that the connection to this Corente Services Gateway is back up before it reverts to this connection. The default is 30 seconds.
- **Packet Loss Threshold:** The minimum percentage of packets that must be lost to cause the partner to detect a failed connection. The default is 100%.

11.9.7.2 Third-Party Devices

If you are configuring a third-party device as a partner, the following settings are available:

- **IKE ID** is an ID that the Corente Services Gateway sends to the third-party device to authenticate using Internet Key Exchange (IKE). You can select one of the following options for the IKE ID:
  - **Name** uses a text string with the domain name and Corente Services Gateway name in the following format: *`domain_name.gateway_name`*
  - **IP Address (WAN)** for Corente Services Gateways in inline configurations, use the WAN IP address. For Corente Services Gateways in peer configurations, use the WAN/LAN IP address.
  - **Specified** lets you define one of the following as an ID:
    - An IP address
    - A string, that is prefixed with the at sign (@). App Net Manager does not send the at sign (@) as part of the IKE identity. For example, if you specify `@ExampleString01`, App Net Manager sends `ExampleString01` as the IKE identity.

> **Note**
>
> The IKE ID is case sensitive and can contain a maximum of 255 ASCII alphanumeric characters including special characters, period or dot (.), hyphen or minus sign (-), and underscore (_). The IKE ID cannot contain embedded space characters.
>
> If you specify the IKE ID, the Peer ID type must be Domain Name on all third party devices. App Net Manager does not support other Peer ID types, such as Email Address, Firewall Identifier, or Key Identifier.

- **Partner IKE ID** is an ID that the Corente Services Gateway receives from the third-party device to authenticate using Internet Key Exchange (IKE). You can select one of the following options for the IKE ID:
  - **WAN IP** for Corente Services Gateways in inline configurations, use the WAN IP address. For Corente Services Gateways in peer configurations, use the WAN/LAN IP address.
  - **IP Address** lets you specify an IP address.
  - **Specified** lets you define one of the following as an ID:
    - An IP address

- A string, that is prefixed with the at sign (@). App Net Manager does not send the at sign (@) as part of the IKE identity. For example, if you specify `@ExampleString01`, App Net Manager sends `ExampleString01` as the IKE identity.

> **Note**
>
> The IKE ID is case sensitive and can contain a maximum of 255 ASCII alphanumeric characters including special characters, period or dot (.), hyphen or minus sign (-), and underscore (_). The IKE ID cannot contain embedded space characters.
>
> If you specify the IKE ID, the Local ID type must be Domain Name on all third party devices. App Net Manager does not support other Local ID types, such as Email Address, Firewall Identifier, or Key Identifier.

- **Timeouts** sets the amount of time, in seconds, before the IKE or IPSec third-party device tunnel needs to be re-established.
  - **IKE Lifetime** - Specifies a timeout value between a minimum of 1,081 and a maximum of 86,400. The default value is `3,600`.
  - **IPSEC Lifetime** - Specifies a timeout value between a minimum of 1,081 and a maximum of 86,400. The default value is `28,800`.
- **Shared Secret** specifies a shared secret used for authenticating to the third-party device using IKE.

11.9.7.3 NAT Settings

The **NAT Settings** section enables you to choose the NAT option for this partner. The setting that you select will apply to this partner only and will interact with the Outbound NAT settings that have been selected for the partner's Default User Group on the partner's Section 11.9.5, “User Groups Tab”. The NAT options are as follows:

- **Prohibited:** This setting prohibits the partner from performing Outbound NAT. When you select this option for the partner, the partner cannot perform Outbound NAT on any of its own subnets that are included in the User Groups being exported to you. No tunnel will be built and a Configuration Alert will be generated if the partner attempts to NAT its own User Groups.

  This option is not supported for third-party device partners.
- **Permitted:** This is a passive setting. The Corente Services Gateway will not NAT this partner's User Groups, but it will not prevent any address ranges from being NATed by the partner. This setting can be overridden by any other NAT setting. This is the default setting.
- **Auto Resolve:** If your Corente Services Gateway detects a conflict between an address range in the local User Groups that you are sharing with the partner and an address range in the partner's User Groups, your Corente Services Gateway will attempt to resolve the conflict by automatically remapping the conflicting remote range to a new address space when this setting is selected. The NATed IP addresses will only be visible by local computers, the remote computers will not know that they have been NATed. When there is no address conflict with the partner, the Auto Resolve setting will function like the Permitted setting. To solve direct address conflicts between two partners, both partners must enable Auto Resolve NAT for each other so that address conflicts are resolved on both sides of the connection. Additionally, both partners can only have Outbound NAT settings of Permitted or Specified in their Default User Group.

  This option is not supported for third-party device partners.

If the local Corente Services Gateway runs out of address space to resolve remote ranges to, the tunnel will not be established and will appear in the Configuration Alert state. An alarm notification will be sent to the email addresses you specify on the Alerts tab, if you choose to be notified about Configuration Alerts. Remember that an administrator cannot control what address ranges will be used when User Groups are NATed using Auto Resolve NAT. If you are concerned about maintaining specific IP addresses for machines on your network or on the networks of remote partners, you can use Inbound NAT to resolve IP address conflicts.

- **Inbound:** This setting can also be used to resolve IP address conflicts. When this setting is enabled for the partner, your Location gateway will remap all IP addresses in the partner's User Groups to a new set of addresses in the subnet that you specify. Unlike Auto Resolve NAT, this setting will remap the addresses even if there are no address conflicts. The NATed IP addresses will only be visible by local computers, the remote computers will not know that they have been NATed. After selecting this option, the adjacent fields will be enabled and must be filled in. Enter the subnet and netmask to which your Location gateway will remap the partner's User Groups. This address space must be unique in your LAN.

  Like the Auto Resolve option, to solve address direct conflicts between two partners, both partners must enable Inbound NAT for each other so that address conflicts are resolved on both sides of the application network connection. Additionally, both partners can only have Outbound NAT settings of Permitted or Specified in their Default User Group.

11.9.7.4 Configuring Tubes

With the Tubes feature, you can organize the secure connection between this Location and its partner into logical tubes that regulate the access of each machine on your LAN to each machine on the remote LAN, and vice versa. Note that a tube does not create a distinct IPSec tunnel for the traffic. A tube is a firewalling mechanism.

At its basic level, a tube is a combination of a local User Group or application, a remote User Group or application, and an optional Firewall Policy that is assigned between them, which definines both the inbound and outbound traffic that the local side will allow over the connection. Each set of partners can have multiple tubes defined for their secure tunnel connection, but each combination of local User Group/application and remote User Group/application can be used in only a single local definition. Tubes can be configured on connections with Intranet Partners, Extranet Partners, and Client Groups, as well as used to define an Internet firewall for the LAN, enable port forwarding of Internet traffic to servers on the LAN, restrict access from the LAN to the Corente Services Gateway, and secure a DMZ.

Tubes are defined separately on both sides of a Location partnership. One side inspects the traffic that it sends, while the other side inspects the same traffic upon receipt. In order for traffic to route properly over the application network, the traffic must match a tube definition on both partners. In other words, for traffic to reach its destination over the connection, the tubes defined on the partner should not conflict with the tubes defined at the local Location gateway. Note that the firewall on tubes is stateful and return traffic is allowed through both firewalls, even if the firewalls usually block that type of traffic.

The Tubes table on the Partners tab lists all of the tubes that you have already configured for this Location in the partnership. If you have multiple tubes, you can rearrange the order in which they are applied to traffic by using the Up and Down buttons. Traffic will attempt to use the tubes in the specific order in which they appear on this table.

You can Edit or Delete any existing tube. To add a new tube, select the Add button. The Add Tube window will be displayed. You can also create new tubes for an existing partner-to-partner connection using the Tube wizard.

Complete the fields in this window as follows:

1. (Optional) Enter a name for your tube in the Tube Display Name field that will help you keep track of this tube's purpose. If you do not enter a name, the tube will be named Tube **num**, where **num** is a number, starting at zero.

2. The Local Side of the Tube section defines the local side of the tube.

   - **User Group:** Select User Group if you would like a local User Group to participate in this tube. Choose the User Group from the adjacent pull-down menu.

     Note

     If you are creating this tube to allow a remote User Group to perform such functions as access the local Corente Services Gateway with Gateway Viewer or monitor it with SNMP, select the Location LAN Address option from the User Group pull-down menu. When selecting a Firewall Policy for this tube, make sure that the following applies:

     - If you are providing remote access to Gateway Viewer, the gateway_viewer Firewall Service must be allowed in this Firewall Policy.
     - If you are monitoring remotely with SNMP, the SNMP Firewall Service must be allowed in this Firewall Policy

     When the User Group option is selected, you can define what traffic you will allow to enter and leave your LAN between the local and remote side. The following Firewall Policy option will be enabled:

     - **Firewall Policy on Tube:** Select a Firewall Policy that you would like to apply to traffic traveling between this User Group and the remote side of the tube.

       Below this option are the following additional fields:

       - **Firewall Policy on User Group:** If there is a Firewall Policy that was enabled when defining the selected User Group and always applies to this User Group, the Firewall Policy will be displayed in this field.
       - **Default Firewall Policy:** The default firewall policy for this type of connection will be displayed in this field. For example, LAN to Remote LAN, LAN to Client, or LAN to Extranet LAN.

       All three Firewall Policies are listed here to remind you that Firewall Policies will be enforced on the connection in this order: Tube Firewall Policy, User Group Firewall Policy, and then Default Firewall Policy.

   - **Application:** Select Application if you would like a local application to participate in this tube. Choose the application from the adjacent pull-down menu.

     For a third-party device, local applications are not supported.

3. The Remote Side of Tube section defines the remote side of the tube. All of the partner's User Groups and applications are listed in the pull-down menus in this section, but depending on the permissions that are granted to you by this partner in its own tube definitions, you may not have access to all of them.

   - **User Group:** Select User Group if you would like a remote User Group to participate in this tube. Choose the remote User Group from the adjacent pull-down menu.

     For a third-party device, choose the Default User Group.

> **Note**
>
> If you want to create a tube to designate a local User Group that is allowed to perform such functions as access the local Location with Gateway Viewer or monitor it with SNMP, select the Location LAN Address option from the remote User Group pull-down menu. You should then select the local User Group that will participate in this tube. When selecting a Firewall Policy for this tube, make sure that the following applies:

- If you are providing access to Gateway Viewer, the gateway_viewer Firewall Service must be allowed in this Firewall Policy .
- If you are monitoring with SNMP, the SNMP Firewall Service must be allowed in this Firewall Policy.

- **Application:** Select Application if you would like a remote application to participate in this tube. Choose the remote application from the adjacent pull-down menu.

  For a third-party device, remote applications are not supported.

4. The Outbound QoS section enables you to enable Quality of Service (Section 10.3, “Quality of Service (QoS)”) settings to the outbound traffic on this tube. QoS settings are viewable and configurable with the Quality of Service feature.

   - **Setting on Tube:** Choose a QoS entry from the pull-down menu to specify the priority of traffic outbound from the Location on this tube.

   > **Note**
   >
   > As when performing any sort of QoS configuration, administrators must be careful when assigning QoS levels because if there is too much high priority traffic, any other traffic with a lower level of priority may become too slow or even be dropped. In addition, you cannot use QoS to prioritize traffic to or from a Corente Client.

   - **Setting on User Group:** If there is an Outbound QoS Setting that was enabled when defining the selected User Group/application and always applies to this User Group/application, the Outbound QoS Setting will be displayed in this field. This field is displayed to remind you that QoS settings will be enforced on the connection in this order: Tube QoS setting and then User Group QoS setting.

5. The Inbound QoS section enables you to enable QoS settings to the inbound traffic on this tube.

   - **Setting on Tube:** Choose a QoS entry from the pull-down menu to specify the priority of traffic inbound from the Location on this tube.

   - **Setting on User Group:** If there is an Inbound QoS Setting that was enabled when defining the selected User Group/application and always applies to this User Group/application, the Inbound QoS Setting will be displayed in this field. This field is displayed to remind you that QoS settings will be enforced on the connection in this order: Tube QoS setting and then User Group QoS setting.

   When you have finished defining the tube, select OK to store your changes or Cancel to close the screen and discard your changes. The new tube will appear in the Tubes table.

Important Notes About Tubes

If traffic from a local User Group or Application tries to reach a remote User Group or Application, it will test each of the tubes defined on the local Corente Services Gateway. If its source, destination, and protocol type are allowed in the definition of any locally defined tube, the traffic will use that tube to reach the remote User Group or Application. The traffic then tests the remotely defined tubes to see if its source, destination, and protocol type are permitted in any of those definitions. This continues until a match is found on both sides. If no match is found, traffic will be treated according to the Firewall Policy of the last tube and whether or not Backhaul has been enabled on the Network tab of the Location form.

It is important that the Firewall Policy of the last tube should be set to Allow if no match on selected Services or Deny if no match on selected Services (rather than Continue). When Continue is selected for the Firewall Policy of a tube, the Corente Services Gateway will continue to try and match traffic to the next tube definition. This becomes a security hazard when applied to the last tube, and could allow unwanted traffic to enter or leave your LAN.

When traffic reaches the last tube without finding a compatible definition, the following applies:

- If Backhaul is enabled, the Corente Services Gateway attempts to match the source address (for outbound traffic) or destination address (for inbound traffic) to an address included in one of the Location's User Groups or applications. If it matches and the address does not have permission to participate in the application network or to send and receive this type of traffic, the traffic is dropped to prevent a security breach. If the address does not match any address in a User Group or used for an application, it is assumed that the user was trying to access the Internet and the traffic is sent to the Backhaul Server, if Backhaul Client is enabled, or to the Internet, if Backhaul Server is enabled.

  It is important to define a Special User Group for Internal Network Description on the User Groups tab for this Location when Backhaul is used, to prevent traffic from being mistakenly sent to non-application-network machines on the LAN rather than the Internet.

- If Backhaul is not enabled, the traffic is unconditionally dropped.

11.9.8 SNMP Tab

The SNMP tab enables you to configure how SNMP will be used to retrieve information about this Corente Services Gateway and its tunnel connections.

To configure SNMP for this Location, fill out this tab as described in the following sections.

- Section 11.9.8.1, “Enable SNMP”
- Section 11.9.8.2, “Contact Information”
- Section 11.9.8.3, “Community Polls”
- Section 11.9.8.4, “Community Traps”
- Section 11.9.8.5, “User Traps”

11.9.8.1 Enable SNMP

Enable SNMP at this Location: When this option is selected, the Corente Services Gateway will become an SNMP-agent and will respond to SNMP 'get' requests to its LAN IP address. It can also be configured to generate SNMP traps that provide alerts about certain alarms and events on the Corente Services Gateway.

11.9.8.2 Contact Information

When SNMP is enabled, click the **Contact Information** button to fill out contact information for this Location.

- **Contact:** Enter the name of the contact for this Location.
- **Street:** Enter the street address of the contact.
- **City:** Enter the city where the contact is located.
- **State/Province:** Enter the state/province where the contact is located, if applicable.
- **Postal Code:** Enter the postal code of the contact, if applicable.
- **Country:** Enter the country where the contact is located.
- **Phone:** Enter the phone number of the contact.
- **Email:** Enter the email address of the contact.

Click OK to store your changes when you are finished.

The tables on the SNMP tab list all of the Community Polls, Community Traps, and User Traps that you have configured for this Location.

11.9.8.3 Community Polls

SNMPv1 and SNMPv2 use **Community Polls** to monitor servers. These polls can also be used to poll this Corente Services Gateway. This section lists all of the community polls that have been configured for this Corente Services Gateway. You can edit or delete any existing polls.

To add a new community poll, select **Add**.

Fill out the screen as follows:

- **User Group (Source Subnet):** Select a User Group that will be allowed to poll this Corente Services Gateway with SNMP v1 or v2 "get" requests to its LAN IP address. You may have to configure special tubes to this Corente Services Gateway containing this User Group.
- **SNMP Community:** If SNMP communities are in use in your implementation of SNMP, enter the community name for this Location in this field. An SNMP Community name functions like a password, because all queries to this Location must use this community name.
- **SNMP View:** Select a view from this list that specifies what MIBs and MIB objects can be retrieved by the User Group (Source Subnet).

When you have completed these fields, click the OK button. This poll definition will be added to the Community Polls list.

11.9.8.4 Community Traps

SNMPv1 and SNMPv2 can also use **Community Traps** to monitor servers. This Location can be configured to send community traps to the SNMP Manager. This section lists all of the community traps that have been configured for this Location. You can edit or delete any existing traps.

To add a new community trap, select **Add**.

Fill out the screen as follows:

- **User Group (Trap Listener):** Select a User Group that will be allowed to listen to this Location to receive SNMPv1/v2 traps. This User Group must contain only one host. You may have to configure special tubes to this Corente Services Gateway containing this User Group.
- **Port:** Enter the port number on the User Group (Trap Listener) to which the Location will send the SNMPv1/v2 traps.
- **SNMP Community:** If SNMP communities are in use in your implementation of SNMP, enter the community name for this Corente Services Gateway in this field. An SNMP Community name functions like a password for SNMP, because all queries to this Corente Services Gateway must use this community name.
- **SNMP Version:** Choose the SNMP version for this trap. You can choose **v1** or **v2c**.
- **Acknowledge Trap:** Select whether or not the User Group (Trap Listener) will acknowledge receipt of a trap by sending a response packet to the Corente Services Gateway. If Acknowledge is selected and the Corente Services Gateway does not receive a response from the User Group (Trap Listener) after a trap is sent, the Corente Services Gateway will wait 30 seconds and send the trap again. The Corente Services Gateway will try three (3) times to send a trap. This option is available only when **v2c** is selected.

When you have completed these fields, click the OK button. This trap definition will be added to the Community Traps list.

11.9.8.5 User Traps

SNMPv3 uses **User Traps** to monitor servers. This Corente Services Gateway can be configured to send user traps to the SNMP Manager. This section lists all of the user traps that have been configured for this Corente Services Gateway. You can edit or delete any existing traps.

Note that unlike SNMP v1 and v2, SNMP v3 is a user-based system. If you would like to poll Corente Services Gateways for information, all that is required to poll any Corente Services Gateway on your application network is a username and password that has been administered on the SNMP Users interface that has appropriate SNMP Views administered. However, if you would like to receive traps with SNMP v3, you must complete the fields and options on this screen.

To add a new user trap, select **Add**.

Fill out the screen as follows:

- **User Group (Trap Listener):** Select a User Group that will be allowed to listen to this Corente Services Gateway to receive SNMPv3 traps. This User Group must contain only one host. You may have to configure special tubes to this Location containing this User Group.
- **Port:** Enter the port number on the User Group (Trap Listener) to which the Corente Services Gateway will send the SNMPv3 traps.
- **Engine ID:** Enter the engine ID of the Trap Listener to help further encrypt the trap. An engine ID is a unique identifier that confirms the identity of both entities when a SNMPv3 trap is sent and received.
- **SNMP User:** Select the user account that will receive these traps.
- **Security Model:** Select the security model that will be used to deliver the traps. **Auth No Priv** will require authentication of the user, but will not encrypt the traps sent to the SNMP Manager. **Auth with Priv** will both authenticate the user and encrypt the traps.

- **Acknowledge Trap:** Select whether or not the User Group (Trap Listener) will acknowledge receipt of a trap by sending a response packet to the Corente Services Gateway. If yes is selected and the Corente Services Gateway does not receive a response from the User Group (Trap Listener) after a trap is sent, the Location gateway will wait 30 seconds and send the trap again. The Corente Services Gateway will try three (3) times to send a trap.

When you have completed these fields, click the OK button. This definition will be added to the User Traps list.

11.9.9 User Remote Access Tab

The User Remote Access tab allows an administrator to manage remote access to this Location for Corente Client users.

11.9.9.1 Client Settings

If you are maintaining legacy Corente Clients, the **Client Settings** section is available.

As of Corente Cloud Services Exchange Release 9.4, you set up Mobile Users for remote access.

11.9.9.2 Mobile User Settings

Administration for both mobile device users and Corente Clients is done using the **Mobile User Settings** section of the User Remote Access tab.

On the User Remote Access tab, in the **Mobile User Settings** section, fill out the following options to allow Mobile User access:

- **Allow Mobile User Access to the Network:** Select this option so that this Corente Services Gateway will serve as a host for Mobile Users.
- **Serve DNS to Mobile Users:** All Mobile Users that connect to this Corente Services Gateway are served IP addressing information by the Corente Services Gateway. This option enables you to select whether or not to pass DNS Server IP addresses with the IP addresses. When this box is selected, Mobile Users will be served the DNS server addresses that you supplied in the **Network** tab of this Locationform.
- **Inactive Session Timeout (min):** Enter the number of minutes that a Mobile User will remain logged into the Corente Services Gateway while the connection is idle before the Mobile User is automatically logged out.
- **Shared Secret:** Enter the shared secret that will be used by the Mobile Users to connect to the Corente Services Gateway. This shared secret will be shared by all the Mobile Users that connect to this Corente Services Gateway.
- **Reserved Address Range:** Enter the address range that will be served by the Corente Services Gateway to the Mobile Users. The address range listed here must have at least one more address than the number of Mobile Users connecting to this Location gateway.
- **Authentication Type:** Specifies one of the following types of authentication:

Local Authentication (Password)	Configures the Corente Services Gateway to authenticate Mobile Users authenticate with user names and passwords. You create the user names and passwords in App Net Manager. The Corente Services Control Point (SCP) then handles authentication and stores the credentials.

External Authentication (RADIUS)	Configures the Corente Services Gateway to authenticate Mobile Users against a RADIUS server on the LAN.
External Authentication (LDAP)	Configures the Corente Services Gateway to authenticate Mobile Users against a Microsoft Active Directory server on the LAN.

Important

Corente Cloud Services Exchange supports only RADIUS servers or Microsoft Active Directory servers as external authentication sources for Mobile Users.

11.9.9.3 Configuring External Authentication

You must specify details for a RADIUS, Active Directory, or LDAP server that resides on your LAN so that the Corente Services Gateway can communicate with the server to authenticate Mobile Users.

Configuring Authentication with RADIUS Servers

To configure authentication with a RADIUS server, do the following:

1. Navigate to the **User Remote Access** tab on the appropriate Location form.
2. Select **Configure** for the **RADIUS Server** option in the **External Authentication Servers** section.
3. Specify values for the following fields:

IP Address	Specifies the IP address of the RADIUS server on your LAN. The IP address must exist in the **Default User Group** for the Corente Services Gateway.
Port	Specifies the port where the Corente Services Gateway connects to the RADIUS server. The default value is 1831.
Secret	Specifies the authentication secret that the Corente Services Gateway uses to connect to the RADIUS server.
Confirm Secret	Validates the authentication secret.
Timeout	Configures the amount of time, in seconds, that the Corente Services Gateway waits for the RADIUS server to respond when authenticating Mobile Users. The default value is 4.
Retries	Configures the number of attempts the Corente Services Gateway makes to authenticate Mobile Users to the RADIUS server. The default value is 2.
Login Prompt	Specifies a prompt that displays to Mobile Users to enter their user names. You can enter any text string with a maximum of 100 characters.
Password Prompt	Specifies a prompt that displays to Mobile Users to enter their passwords. You can enter any text string with a maximum of 100 characters.

4. Select **OK** to save and close the RADIUS server configuration.
5. Select **OK** on the Location form to save your changes.

Configuring Authentication with Microsoft Active Directory

Important

The following requirements apply to using Microsoft Active Directory (AD) servers for external authentication:

- Server Message Block (SMB) signing is required. You must enable SMB signing on the AD server.
- Mobile User names that you define in App Net Manager must match the user names that you define in AD.
- Password expiration polices that you define in App Net Manager do not apply to user accounts in AD.

To configure authentication with a Microsoft Active Directory (AD) server, do the following:

1. Navigate to the **User Remote Access** tab on the appropriate Location form.
2. Select **Configure** for the **LDAP Server** option in the **External Authentication Servers** section.
3. Specify values for the following fields:

IP Address	Specifies the IP address of the AD server on your LAN. The IP address must exist in the **Default User Group** for the Corente Services Gateway.
NetBIOS Name	Specifies the NetBIOS identifier of the AD server on your LAN. You must specify the NetBIOS name if you specify an IP address.
DNS Name	Specifies the domain name of the AD server on your LAN. The server must exist in the **Default User Group** for the Corente Services Gateway.
User Name	Specifies the user name that the Corente Services Gateway uses to authenticate against the AD server. This user account must be a member of the **Account Operators** group in the AD server.
Password	Specifies the password that corresponds to the user name.
Base	Specifies the distinguished name (DN) of the search base object in your directory.

4. Select **OK** to save and close the server configuration.
5. Select **OK** on the Location form to save your changes.

Configuring LDAP Authentication (Legacy Versions Only)

If your Corente Services network includes legacy versions of the Corente Client, you can maintain your LDAP configuration.

To maintain your legacy LDAP configuration, do the following:

1. Navigate to the **User Remote Access** tab on the appropriate Location form.

2. Select **Configure** for the **LDAP Server** option in the **External Authentication Servers** section.
3. Specify values for the following fields:

IP Address	Specifies the IP address of the LDAP server on your LAN. The IP address must exist in the **Default User Group** for the Corente Services Gateway.
NetBIOS Name	Specifies the NetBIOS identifier of the LDAP server on your LAN. You must specify the NetBIOS name if you specify an IP address.
DNS Name	Specifies the domain name of the LDAP server on your LAN. The server must exist in the **Default User Group** for the Corente Services Gateway.
Port	Specifies the port number that the Corente Services Gateway uses to connect to your LDAP server. The default value is 389.
Backup LDAP Server	Specifies the location for a secondary, or failover, LDAP server on your LAN.
User Name	Specifies the user name that the Corente Services Gateway uses to authenticate against the LDAP server.
Password	Specifies the password that corresponds to the user name.
Timeout	Configures the amount of time, in seconds, that the Corente Services Gateway waits for the LDAP server to respond when authenticating Mobile Users. The default value is 4.
Base	Specifies the distinguished name (DN) of the search base object in your directory.
Scope	Configures the starting point for directory queries. You can select one of the following: • **Base** queries the base object only. • **One Level** queries objects subordinate to the base object but does not include the base object. • **Subtree** queries the base object and entire subtree of the directory for which the base object is the highest object.
Filter	Specifies entries to allow or exclude from directory queries.
Attributes	Specifies attribute values to match in directory queries.

4. Select **OK** to save and close the RADIUS server configuration.
5. Select **OK** on the Location form to save your changes.

11.9.10 High Availability Tab

If a Corente Services Gateway becomes unreachable by its partners due to connection, router, or local loop problems, you can provide alternate methods for partners to reach each of the Location's User Groups and applications. This is referred to as Traffic failover, which can be configured on the High Availability tab.

To use traffic failover, choose one or more Corente Services Gateways in your application network to function as a Backup Location gateway for each User Group and application of this Location gateway, known as the Primary Corente Services Gateway. If a tunnel or connection fails to the Primary Corente Services Gateway, users at the partner Locations can continue to access necessary corporate resources by utilizing a tunnel to the Backup Corente Services Gateway.

Important

A Primary Corente Services Gateway and its Backup Corente Services Gateways must never be configured as application network partners.

Traffic failover can be arranged as follows to provide high availability for the connections in your application network:

- **Collocated Primary and Backup Location Gateways**

  Traffic failover can be used to provide an entirely redundant connection to a LAN. In this scenario, the Primary and Backup Corente Services Gateways are installed on the same LAN, but connected to separate WAN routers, separate physical local loops, and separate carrier clouds. If the Primary Corente Services Gateway becomes unreachable because one or more of these elements fail, remote sites connecting to the Primary Corente Services Gateway can fail over to their connections to the Backup Corente Services Gateway. Additionally, all computers on the LAN participating in the application network automatically reroute to the Backup Corente Services Gateway for application network access, as well.

- **Primary and Backup Location Gateways on Different LANs**

  Enterprises can use traffic failover to recover in the event that a hub site goes down. If a hub site fails, the remote sites can use one or more Backup Corente Services Gateways located at one or more other sites to reach their necessary subnets and resources. The site of a Backup Corente Services Gateway may contain the same necessary resources that the main hub site contained (for example, if it is a mirror site or disaster recovery center) or the site of the Backup Corente Services Gateway may have routing infrastructure that can route to the Primary Corente Services Gateway's LAN through alternate means (such as a frame relay service, ATM, or private line).

In both scenarios, for partners to use a Backup Location gateway's tunnel to connect to computers behind the Primary Corente Services Gateway, routers must be in place behind both the Primary Corente Services Gateway and the Backup Corente Services Gateway. The router behind the Primary Corente Services Gateway must be configured with alternate routes for application network traffic to the Backup Corente Services Gateway, while the router behind the Backup Corente Services Gateway must be configured to recognize the subnets behind the Primary Corente Services Gateway and route any traffic destined for those subnets to the appropriate location. The location can be either mirrored subnets or the real subnets, if a non-application-network connection to the Primary Location gateway's LAN is present.

Additionally, partners of the Primary Corente Services Gateway must also be partners of the Backup Corente Services Gateway, so that if tunnels to the Primary Corente Services Gateway fail, the partners can reach the Primary Corente Services Gateway's LAN or mirrored subnets through their tunnels to the Backup Corente Services Gateway. Remember, though, that a Primary Corente Services Gateway and its Backup Corente Services Gateway must never be configured as application network partners.

User Group Failover Settings

In this section, specify the general parameters that will apply to traffic failover for this Primary Corente Services Gateway. On the Section 11.9.7, “Partners Tab”, you can specify settings for each partner that will override these settings.

- **Failover/Failback detection interval (secs):** The period of time that the partner of this Corente Services Gateway will wait until it fails over to a Backup Corente Services Gateway when it detects that the connection to this Corente Services Gateway is down. Also, the period of time that the partner will wait after it detects that the connection to this Corente Services Gateway is back up before it reverts to the connection to this Corente Services Gateway. The default is 30 seconds.
- **Packet Loss Threshold (percent):** The minimum percentage of packets that must be lost to cause the partner to detect a failed connection. The default is 100%.

Add/Edit Failover Locations

Corente Services Gateways can have failover Locations. Failover Locations provide backups for Corente Services Gateways. If a Corente Services Gateway becomes unavailable, the partners for that Corente Services Gateway connect to the failover Location.

Partner Corente Services Gateways connect to one failover Location at a time. However, you can configure user groups and applications for partners so that they use different, multiple failover Locations.

Use the **Up** and **Down** buttons to arrange failover Locations by order of priority.

To add a new failover configuration, click the **Add** button.

Fill out the fields as follows:

- **Failover Location:** Select the Corente Services Gateway from this pull-down menu that you would like to function as the Backup Corente Services Gateway. This menu will contain every Location in your application network that is not a partner of this Corente Services Gateway.
- **Select User Groups/Applications for Failover:** Choose the User Groups and applications that will use the selected Location as a Backup Location gateway. When a Backup Corente Services Gateway is being used for failover, all User Groups and applications that you choose here will use that Corente Services Gateway to reach necessary resources.

When you have finished, click the **OK** button to store your changes or the **Cancel** button to discard your changes.

Load Balancing with Failover

If you would like to let hub sites with multiple Location gateways manage application network traffic by allowing these Corente Services Gateways to support the same User Groups and applications, you can use the High Availability tab in conjunction with the Partner for Failover Only option on the Section 11.9.7, “Partners Tab”. Select this option to use a Corente Services Gateway partner as a Backup connection to a site if the connection to the Primary Corente Services Gateway partner at that site should fail.

To use this option, begin by configuring the Primary and Backup Corente Services Gateways for a hub site. Each Corente Services Gateway requires a separate, distinct personality file, but the personality files can include identical User Group and application definitions. Both the Primary and Backup Corente Services Gateways of the hub site should be partnered with the Locations that must connect to this site. Additionally, the Primary Corente Services Gateway must have the Backup Corente Services Gateway selected as the Backup Corente Services Gateway on its High Availability tab for one or more User Groups/applications.

Next, when configuring the Locations that must connect to this site, select both the Primary and Backup hub site Location gateways as partners, but select the Partner for Failover Only option for the Backup Corente Services Gateways. This Location will now connect to the hub site through the Primary Corente Services Gateway until a failure scenario occurs, and then will be able to connect to the same site through the Backup Corente Services Gateway.

Traffic Failover and Automatic Routing Protocols

Some considerations must be made when enabling traffic failover and automatic routing protocols (such as RIP, OSPF, and BGP) at the same time in a datacenter. To illustrate, consider the example of Gateway A and Gateway B, located within the same datacenter, and Gateway C, which is located at another site.

In the simplest case, Gateway A is partnered with Gateway C. Gateway B is partnered with Gateway C as a Partner for Failover Only, for a backup route to the datacenter. As failover (or failback) occurs, routes for Gateway C are automatically advertised on Gateway A or Gateway B (whichever is currently up). Advertisement of new RIP, OSPF, and BGP routes will be automatic; just ensure that the autorouting protocol you are using (RIP, oSPF, or BGP) is turned on for the routers at the datacenter.

However, if Gateway A and Gateway B are both ordinary partners of Gateway C (in other words, neither is Partner for Failover Only), and Gateway B is configured as a backup for Gateway A's applications and subnets on Gateway C, the same automatic advertisement will not work because Gateway A and Gateway B are in the same datacenter. You can only have one gateway (A or B) communicate with Gateway C at a time, because routes will be advertised on the LAN from both A and B to C at the same time. This can be resolved by weighting the RIP, OSPF, and BGP routes so that Gateway A is favored, in which case, failover and auto-advertisement of routes will occur correctly.

11.9.11 Alerts Tab

Occasionally, Corente Cloud Services Exchange may need to notify you about problems or events that occur with this Corente Services Gateway. The Alerts tab is used to configure your preferences for these alerts. These alerts can be delivered in the form of notification emails to the addresses that you specify and SNMP traps. One or more notification methods may be unavailable for each type of alert, depending on how you have configured this Location.

Note that you can view Active Alarms, Cleared Alarms, and Events that have been generated in this domain (and specifically from this Location) with the Alarms and Events feature in App Net Manager. You will also be able to view Active Alarms generated by Locations and tunnel connections on the map.

To configure alerting for this Location, fill out the following sections of this screen:

- Email Addresses to Receive Alerts
- Tunnel Alarms
- System Alarms
- Alarm Email Suppression

Email Addresses to Receive Alerts

In this section, you can either select the Use Default Emails option defined in the Preferences option, to use the default email addresses that you supplied in the domain contact information, or manually specify email addresses that will receive the alerts. You can edit or delete any existing email address in the email list.

To add a new email address, select the **Add** button, enter the address, and then click the **OK** button to store your addition.

Tunnel Alarms

This section contains the following options:

- **Notify on configuration alerts:** When this option is selected, the service will send an email notification and SNMP trap if a User Group of this Location has a configuration problem. Your Location and its tunnel connections will remain disabled until the configuration problem has been resolved. If this option is not selected, the service will not send a notification email or SNMP trap when this event occurs. The following configuration problems would cause this alert:
  - This Location's User Groups contain nested subnets, within themselves or within a Location partner's User Groups, and the Allow Locations to be configured with nested subnets option is unchecked on the Section 11.9.2, “Network Tab”.
  - The User Groups of this Location overlap with the User Groups of one of its partners and no NAT options have been selected by this Location or its partners.
  - The User Groups of this Location overlap with the User Groups of one of its partners and the wrong NAT options have been set on this Location or its partners.
- **Notify on loss of tunnel to SCP:** When this option is selected, the service will send an email notification and SNMP trap if this Location becomes disconnected from the Corente SCP. If this option is not selected, the service will not send a notification email or SNMP trap when this event occurs. The email will be sent according to the threshold that you have chosen with the Duration of connection loss before receiving email notification pull-down menu.
- **Notify on loss of tunnel to Partners:** When this option is selected, the service will send an email notification and SNMP trap if this Location becomes disconnected from any of its Location partners. The email will be sent according to the threshold that you have chosen with the Duration of connection loss before receiving email notification pull-down menu. If this option is not selected, the service will not send a notification email or SNMP trap when this event occurs.
- **Duration of connection loss before receiving email notification:** This option allows you to set the length of time before an email notification is triggered, ranging from immediate notification to notification only after 8 hours of downtime. You may also choose to never be notified.

  The benefit of immediate notification is that you can respond to any problems as soon as they occur; however, a longer delay prevents unnecessary notifications. For example, your ISP may have an interruption of service for 5 minutes and then re-establish your Internet connection. If you have chosen to be notified immediately, you would receive an email even though Internet connection is re-established quickly. If you have chosen to be notified in 1 hour, by which time the Corente Services Gateway has reconnected to the Corente SCP and its partners, you would avoid this email.

System Alarms

This section contains the following options:

- **Notify on Software Upgrade:** When this option is selected, the service will send an email notification if a software upgrade has occurred. When this option is unselected, no email notifications will be sent when the software is upgraded, even if a reboot of the Corente Services Gateway is required. You cannot choose to be notified of this alarm by an SNMP trap.
- **Notify on Failover:** When this option is selected, the service will send an email notification and SNMP trap if a hardware switch (when using Redundant Hardware) or traffic failover has occurred for this Corente Services Gateway. If this option is not selected, the service will not send a notification email or SNMP trap when this event occurs.
- **Notify on Security Alert:** When this option is selected, the service will send an email notification and SNMP trap if a security alert occurs on this Location or one of its tunnels. If this option is not selected, the service will not send a notification email or SNMP trap when this event occurs.

Alarm Email Suppression

This section enables you to suppress email alerts during regularly scheduled maintenance periods for your network.

Complete the fields in this section as follows:

- **Duration:** Select the period of time for which email notifications will be suppressed, between 1 hour and 9 hours. When Duration is set to None, Alarm Email Suppression will be disabled.
- **Frequency:** Select the frequency of alarm email suppression. Choose a day, Daily or any single day of the week. Choose a time, any hour of the day.

Depending on what maintenance is routinely performed, you may only need to disable certain email alarms from this gateway. Choose one or more of the following:

- **Application Alarms:** Select this option to disable all email notifications concerning applications.
- **Server Alarms:** Select this option to disable all email notifications concerning servers.
- **Tunnel Alarms:** Select this option to disable all email notifications concerning tunnels.

11.9.12 Hardware Info Tab

The Hardware Info tab displays information about the computer running the Corente Services Gateway.

This tab includes details of the following:

- Hardware manufacturer and serial number
- Memory
- Hard disks
- CPU
- Network Interfaces

11.10 Location States

The **Detail** tab displays states for the Corente Services Gateway software and clones of the Corente Services Gateway software. Clones preserve the current version of the software in partitions on the host storage. If a Corente Services Gateway cannot upgrade successfully, it automatically reverts to the cloned version.

The following table describes states for the Corente Services Gateway software:

State	Description
INITIAL	The Corente Services Gateway has started for the first time.
UNKNOWN	The Corente SCP cannot determine the state of the Corente Services Gateway. This generally occurs when software upgrades fail.
STAGING	A software upgrade is in the process of being loaded in a new partition.
STAGED	A software upgrade is loaded on the partition.
ARMED	A software upgrade will occur on the next reboot.

State	Description
BOOTING UP	The software upgrade has occurred and the Corente Services Gateway is starting but has not yet connected to the Corente SCP.
WORKS	The software upgrade was successful. The Corente Services Gateway has connected to the Corente SCP at least once.
FAILED	The software upgrade was not successful. The Corente Services Gateway uses the clone partition to automatically restore the previous software version.

Chapter 12 Creating Location Partners

Location partners are configurations that allow traffic between Corente Services Gateways. You establish Location partners by adding tubes from one Location to another Location. The tubes provide a secure connection between the Location partners to allow access to user groups and applications.

You create Location partners to set up intranets and extranets in your Corente Services network.

Intranets	Secure connections between Corente Services Gateways in the same Corente Services domain.
Extranets	Secure connections between Corente Services Gateways in different Corente Services domains. When you create extranets, you export your Locations to the other domain and then import the Locations from that domain. You must then create Location partner configurations between those Locations. For more information, see Creating Extranets.

In addition to creating intranets and extranets, you can create partner configurations between Corente Services Gateways and Mobile User Groups, third-party devices, or legacy Corente Clients. These configurations allow Mobile Users and third-party devices to connect to your Corente Services network. However, the process of configuring a Mobile User Group or third-party device as a Location partner is the same as for configuring Corente Services Gateways.

Overview for Creating Location Partners

The following is an overview of the process for creating Location partners:

1. Select **File** then **Wizards** and then **Partner Locations** to launch the **Add Location Partners** wizard.
2. Select two Locations in your Corente Services domain to add to the partner configuration.
3. Define tube settings for the first Location in the partner configuration.
   a. Select a user group or application that is local to the first Location. This is the user group or application that you want to make available to the other Location in the partner configuration. You add a tube that allows the other Location to access that user group or application.
   b. Select a firewall policy for the tube.

      Tubes are firewall mechanisms, not separate IPSec tunnels. When you add a tube to the Location partner configuration, you can optionally select a firewall policy to apply to traffic on the tube. If you apply a firewall policy to the tube, it takes priority over the default firewall policy as well as any firewall policy that you define for specific user groups or applications.
   c. Select a user group or application on the remote Location. The remote Location is the second Location in the partner configuration. The user group or application that you select is the one that you want to make available to the first Location in the partner configuration.
   d. Configure inbound and outbound Quality of Service (QOS) settings. You can optionally select QOS rules so that the Corente Services Gateways apply to inbound and outbound traffic on the tube.
4. Define matching tube settings for the second Location in the partner configuration.
5. When prompted, select **Finish** to exit the **Add Location Partners** wizard and then save your changes to the Corente SCP.

6. Configure additional settings for the partner configuration.
   a. Expand the **Locations** folder in the domain directory.
   b. Right-click the first Location in the partner configuration and select **Edit**.
   c. Select the **Partners** tab.
   d. Select the Location partner that you created and then select **Edit**.
   e. Define connection, failover, and NAT settings as appropriate.
   f. Select **OK** and save your changes to the Location configuration.
   g. Make the corresponding changes to the second Location in the partner configuration.
   h. Save your changes to the Corente SCP.

Related Information.

- Section 11.9.7, “Partners Tab”
- Section 11.9.7.4, “Configuring Tubes”

Chapter 13 Creating Extranets

Table of Contents

Extranets let you establish secure connections between Locations in your domain and Locations in another Corente Services domain.

The purpose of an extranet is to share access to resources between domains. When you create an extranet, you select User Groups and Applications on specific Locations in your domain that devices on the other domain can access.

Note

You cannot change the configuration of Locations in other domains.

Extranets use a model of mutual consent. The following is an overview of the process to create an extranet:

1. You export Locations in your domain to another domain. The administrator of the other domain exports Locations to your domain.
2. You import the Locations that the other administrator exported. The administrator of the other domain imports the Locations that you exported.
3. You add Location Partners between Locations in your domain and Locations in the other domain. The administrator of the other domain adds corresponding Location Partners.

As you go through each step to create an extranet, the **Detail** tab displays the following statuses in the **Import Status** column:

Import Status	Description
Unavailable for Import	The administrator in the other domain has not yet exported Locations to your domain. This is the initial status when you export Locations from your domain. After you save changes in App Net Manager to the Corente SCP, and the other administrator exports Locations to your domain, the status updates to **Available for Import**.
Available for Import	The administrator on the other domain has exported Locations to your domain. You can now import those Locations to your domain.
Imported	You have successfully imported Locations from the other domain. You can now create Locations Partners with that domain.

13.1 Exporting Locations to Other Domains

The first step in creating an extranet is to export Locations in your domain to another domain. You select User Groups and Applications in specific Locations in your domain to which you want to provide access.

To export one or more Locations in your domain to another domain, do the following:

1. Right-click **Extranet Imports/Exports** in the domain directory and then select **Add Export**.

   The **Export to Domain** dialog displays.

2. Specify the domain to which you want to export Locations from the **Export to Domain** menu.

   Important

   You can enter a domain name if it is not available from the menu. However, you must enter the domain name exactly as the other administrator has configured it in App Net Manager.

3. Select **Add** to choose a Location in your domain to export.

   The **Export Location** dialog displays.

4. Select the Location to export from the **Exported Location** menu and then select the User Groups or Applications to export.

5. Select **OK** to close the **Export Location** dialog.

6. Select additional Locations to export, if required, and then select **OK** to close the **Export to Domain** dialog.

   The domain status displays as **Unavailable for Import**.

7. Select **File** and then **Save** to save your changes to the Corente SCP.

13.2 Importing Locations from Other Domains

Importing Locations from another domain allows you to connect with the User Groups and Applications in that other domain.

To import Locations from another domain, do the following:

1. Select **Extranet Imports/Exports** in the domain directory.

2. Right-click the domain that you want to import and then select **Import Domain**.

   The domain status changes from **Available for Import** to **Imported**.

3. Select **File** and then **Save** to save your changes to the Corente SCP.

After you import an Location from another domain, it displays on your map and in the **Locations** folder with the following icon: 

Note

You cannot arrange the position of extranet Locations on the map.

13.3 Creating Location Partners in an Extranet

To connect Locations in an extranet, launch the **Partner Locations** wizard and follow the steps to create Location Partners. Alternatively you can edit the Location in your domain and complete the details on the **Partner** tab.

The administrator of the other domain must also create corresponding Location Partners so that the Tubes between Locations in the extranet match each other. For example, you select the **Auto Resolve** option in the network address translation (NAT) settings when you add an extranet Location as a Partner for a Location in your domain. In this case, the administrator in the other domain must also select the **Auto Resolve** option when adding the Location imported from your domain as a Location Partner.

Related Information. Creating Location Partners

13.4 Revoking Imported Domains

Revoking a domain that you have imported temporarily suspends the extranet with that domain. The secure connection between domains is taken down and Locations in the extranet can no longer access resources in the corresponding domains. Locations that are imported into other domains are removed from the domain map and **Locations** folder.

To revoke an imported domain, do the following:

1. Select **Extranet Imports/Exports** in the domain directory.
2. Right-click the domain that you want to revoke and then select **Revoke Domain Import**.

   The domain status changes from **Imported** to **Available for Import**.
3. Select **File** and then **Save** to save your changes to the Corente SCP.

To restore the extranet after revoking the imported domain, you must import the Locations and create the Location Partners again.

Chapter 14 Adding Third-Party Devices

Corente Cloud Services Exchange supports certain third-party devices.

To add a supported third-party device, do the following:

1. Right-click **3rd-Party Devices** in the domain directory and then select **Add 3rd-Party Device**.

   The **Add 3rd-Party Device** dialog displays.

2. Specify values for the appropriate fields. See Third-Party Device Settings.
3. Select **OK** to close the **Add 3rd-Party Device** dialog.
4. Select **File** and then **Save** to save your changes to the Corente SCP.

Third-Party Device Settings

The following fields are available on the **Add 3rd-Party Device** dialog:

Name Specifies a unique identifier for the third-party device.

Type Specifies the manufacturer of the third-party device.

Model Specifies the model of the third-party device.

Notes Specifies additional details about the third-party device.

WAN IP Address Specifies the IP address of the third-party device on the wide area network (WAN).

Visible IP Address Specifies the IP address of the third-party device that is externally visible on the public Internet.

Backhaul Configures the third-party device as a backhaul server.

Note

- Third-party devices that you configure as backhaul servers uses a subnet of `0.0.0.0` by default.
- If you configure the third-party device as a backhaul server and then add it as a Partner for a Location, then that Location cannot have any other Partner. The Location routes all LAN traffic to the third-party device.

  Devices that are behind the third-party device can communicate directly with the Location, or Corente Services Gateway. As a result, you cannot access Gateway Viewer or use SNMP to monitor the Corente Services Gateway through the backhaul tunnel.

Compression Configures the third-party device to compress data to improve network performance. In most networks this setting is not required.

DPD	Configures the third-party device to use Dead Peer Detection (DPD).
PFS	Configures the third-party device to use Perfect Forward Secrecy (PFS).
NATT	Configures the third-party device to use Address Translation Traversal (NAT-T).
IKE Options	Specifies the Internet Key Exchange (IKE) cryptographic protocols that the third-party device uses. You should not modify the default setting.
ESP Options	Specifies the Encapsulating Security Payload (ESP) cryptographic protocols that the third-party device uses. You should not modify the default setting.
Subnets	Specifies the subnets in your Corente Services network that can connect to this third-party device. • **Network Address** sets the first IP address in the subnet. • **Subnet Mask** defines the range of IP addresses in the subnet.

Chapter 15 Working with Reports

Table of Contents

App Net Manager reports information about your domain in graphs that show performance metrics and log files that capture system and administrator activity.

To work with reports, you can right-click graphs and logs in the domain directory and then select:

- **Refresh/Clear Changes** to load the most recent data and delete any unsaved changes.
- **Save To File** to save the data to your local filesystem.
- **Email** to forward as an email.

Note

You should configure default mail server (SMTP) settings in your domain preferences first.

Related Information. Configuring SMTP Server Settings

15.1 Graph Categories

App Net Manager provides the following graph categories:

Bandwidth	Bandwidth graphs show the bits-per-second capacity for inbound and outbound traffic to and from Locations in your domain.
Partners	Partners graphs display information about Location Partners.
Applications	Applications graphs display information about application servers that you have added to Locations.
Servers	Servers graphs display information about monitored servers that you have added to Locations.

15.2 Log Categories

App Net Manager provides the following log categories:

Administration

Administration logs capture information about activity from the following users:

- **Super User** is the root administrator account.
- **SCP Operator** is the user who operates and administers the Corente Services Control Point (SCP).

- **External** is an external administrator account.
- **End User** is a Corente Client user account.

If you have additional local administrator accounts in your domain, App Net Manager also captures information about those users.

Application Server Status

Application server status logs capture information about the application servers that you have added to Locations in your domain.

See Table 15.1, “Application and Server Status”

Application Status

Application status logs capture changes to applications in your domain.

See Table 15.1, “Application and Server Status”

Client

Client logs capture information about the Corente Clients that connect to Locations in your domain.

Hardware Failover

Hardware failover logs capture information when failover occurs for Locations that are configured for redundant hardware.

The **Scheduled** field indicates if the failover was planned or due to a hardware issue. **Yes** indicates that the failover occurred during the scheduled maintenance window for software upgrades. **No** indicates that the failover occurred due to a hardware issue with the primary instance of the Location.

Host Status

Host status logs capture information about the monitored servers that you have added to Locations in your domain.

See Table 15.1, “Application and Server Status”

Traffic Failover

Traffic failover logs capture information when User Group failover occurs in your domain.

Applications and servers can have the following statuses:

Table 15.1 Application and Server Status

Status	Description
Up	The application or server is currently active and available.
Down	The application or server is not currently active or available.
Unknown	It is not currently possible to connect to the application or server.
Warning	One of the following: • The application or server has exceeded the warning threshold that you defined when you added the application or server in App Net Manager. • The application or server is failing diagnostic tests for certain protocols.
Critical	The application or server has exceeded the critical threshold that you defined when you added the application or server in App Net Manager.
N/A	App Net Manager is not configured to perform diagnostic tests on the application or server.

15.2.1 Filtering Logs

To filter log details, do the following:

1. Open any log file from the **Logs** folder in the domain directory.
2. In the **Detail** tab, select the detail by which you want to filter the log entries.
3. Select one of the following:
   - **Filter in** to show only log entries that include the detail.
   - **Filter out** to hide any log entries that include the detail.
4. Select **Reset** to clear the filter and show all log entries.

15.3 Custom Reports

Depending on your requirements, your Corente SCP operator can make additional reports available, as follows:

All Clients in Domain	Displays information about all Corente Client user accounts in the domain.
All Location Routes in Domain	Displays information about all routes between subnets on the local network and the Corente Services Gateways in the domain.
All Location Routes in Domain	Displays information about all routes between subnets on the local network and the Corente Services Gateways in the domain.
All Location to Location Tubes in Domain	Displays information about all tubes that exist between Locations in the domain, including tubes to Locations you import from other domains.
All Location User Groups in Domain	Displays information about all User Groups and applications in each Location in the domain.
Client Partnership Detail	Displays information about partner configurations between Corente Clients and Locations.
All Locations in Domain	Displays information about all Locations in the domain. This report includes states for the Corente Services Gateway software and clones of the Corente Services Gateway software. See Section 11.10, “Location States”.

Chapter 16 Working with Alarms and Events

App Net Manager generates alarms and events to notify you when system and configuration changes take place or if issues occur with your Corente Services network.

Alarms are notifications for changes that affect the system and require your attention. Active alarms currently affect the system. When the system detects that the issue is resolved, or no longer applies, it automatically clears the alarm. Cleared alarms display for 30 days.

Events are informational notifications about system changes that have occurred.

To work with alarms and events, you can:

- Double-click them to view detailed information.
- Right-click them and then select **Email** to forward as an email.

> **Note**
>
> You should configure default mail server (SMTP) settings in your domain preferences first.

- Right-click the containing folders and then select **Sort Alarms/Events** to arrange the order in which the alarms and events display. The following options are available:
  - **By Day** sorts alarms and events by date and time. Select this option to view the most recent alarms and events first. This is the default option.
  - **By Class** sorts alarms and events by type. Select this option to view the most severe or critical alarms and events first.
  - **By Code** sorts alarms and events by identifier. Select this option to group similar alarms and events.
  - **By Source** sorts alarms and events by the object that caused them. For example, if a configuration change causes a Location to restart, that Location is the source of the alarm or event.

Related Information.

- Section 7.1.3, “Loading and Refreshing Alarms”
- Configuring SMTP Server Settings

Part II Gateway Viewer Help

The *Gateway Viewer Help* is available from the **Help** menu item in Gateway Viewer. However, the help content for Gateway Viewer is also included in this part of the *Corente Services Administration Guide* for your reference.

Table of Contents

Chapter 17 Gateway Viewer

Table of Contents

17.1 Introduction to Gateway Viewer

This is the Gateway Viewer application. The Gateway Viewer allows you to access both local and remote computers as well as perform certain network administration tasks using a web browser and Ethernet connection to your local Corente Services Gateway.

The Gateway Viewer uses SSL for secure access to the Corente Services Gateway. When you access the Gateway Viewer, you will be asked to accept a certificate, signed by Corente. Although this certificate will not be signed by a trusted authority, you must accept the certificate to provide encryption to the Corente Services Gateway.

Note

If you are using Internet Explorer 9.0 or later, you will be alerted that the certificate does not appear to be valid. Select **Continue Anyway** to access Gateway Viewer without harm to your system.

The application is accessible via buttons displayed across the top of the browser window. Each button presents a menu of options upon mouse rollover.

- **Monitoring Application** allows you to monitor the applications and/or servers that are provided to you by local and remote Corente Services Gateways. This button will be available only if you have subscribed to either application monitoring or server monitoring.
- **Networks** allows you to connect to both local and remote computers.
- **Help** displays this Gateway Viewer help file.
- **Admin Login** allows you to login to the Gateway Viewer application as an administrator. The following additional buttons are available if you have logged in:
  - **Monitoring Top Talkers** allows you to monitor bandwidth usage by individual users on a network.
  - **Network Admin** provides you with tools to manage the connections that this Corente Services Gateway provides.
  - **Gateway Admin** allows you to manage this Corente Services Gateway.
  - **Logout** logs you out of the Gateway Viewer, so that only the user interface is displayed.

In general, do not use the **Refresh** button on your browser to refresh a page in Gateway Viewer. To view the most up-to-date information for any page that you are viewing, right-click your mouse button within the bottom frame of the page and select the **Refresh** option from the menu that appears. This will cause the appropriate frame on the page to reload with the most recent data.

Note

Occasionally, when you attempt to load a page in Gateway Viewer, the menu in the top frame of the page may disappear. If this occurs, simply close your browser window. You should then open a new browser window and re-access Gateway Viewer.

17.1.1 Supported Browsers

The Gateway Viewer application supports the following browsers:

- Microsoft Internet Explorer 9.0 or later
- Mozilla Firefox 25.0 or later
- Google Chrome 34.0 or later
- Apple Safari 7.0 or later

Note

- You can browse file servers from Gateway Viewer only if you use Microsoft Internet Explorer.
- You can connect to Gateway Viewer only from a running instance of Corente Services Gateway on your local area network (LAN).

17.2 Admin Login

Gateway Viewer is intended for use by both users and administrators of the secure application network.

- For users, Gateway Viewer provides an interface for connecting to both local and remote computers as well as checking the status of applications that can be used locally and over the secure network.
- For administrators, Gateway Viewer provides localized control over the Corente Services Gateway, a platform for monitoring network usage, and information that can aid in problem drill-down and diagnosis. To prevent users from gaining access to the administrative interface, a login is required.

Before logging in, by default, the only buttons available in the Gateway Viewer toolbar are **Monitoring** (if subscribed to), **Networks**, **Admin Login**, and **Help**.

To access the administrative features of Gateway Viewer, you must select the **Admin Login** button. When you enter the Gateway Viewer user name and password and click **OK**, the complete set of Gateway Viewer features will be available for use. When you have finished using the administrative features of Gateway Viewer, you should logout of the application by selecting the **Logout** button.

17.3 Monitoring

Monitoring allows you to view statistics and graphs about applications and servers within your application network, as well as data about bandwidth usage by individual machines.

- **Application**
  - **Application monitoring** allows your company to deploy applications easily between sites within your application network. Simply register the application with the local Corente Services Gateway in App Net Manager, and you can share the application securely (like a User Group) with any other Corente Services Gateway within your intranet or extranet. Application monitoring was designed with the following principles in mind: to confirm to both users and administrators that the applications are functioning correctly; to facilitate communication between both parties when they are not; to provide reports to help with capacity planning; and to provide diagnostic capabilities to locate bad actors within the network.
  - **Server monitoring** allows local administrators to monitor local servers. Simply register the server(s) with the local Corente Services Gateway in App Net Manager, and you can view usage statistics about each server concerning CPU, disk space, physical memory, and/or swap space.
- **Top Talkers** allows an administrator to monitor network activity between machines on the local network and machines at remote sites and/or the Internet, to identify what machine pairs are using up the most bandwidth (i.e., the "top talkers").

The features that are available on the Monitoring screen(s) depend on whether or not you have logged in to Gateway Viewer via the Admin Login.

17.3.1 User Interface

The **User Interface** of **Monitoring** will be displayed if you have not logged into Gateway Viewer via the **Admin Login** button. This interface allows users to view the status of each application that is available on local and remote networks, and to communicate with the specific administrator of each application via email. This interface will be available only if you have been permitted access to an application from a network that has subscribed to the application monitoring service. Depending on the permissions that the user's IP address has been granted via tubes in App Net Manager, this page may not be available or applications that appear on this page may not be accessible. If unsure, users should contact their administrators to determine what applications they have been permitted to access. The tables on this interface can be sorted via any category simply by selecting that category's heading. The category that is currently used for sorting will be displayed in bold characters. By default, the tables will be sorted alphabetically by the **Application** category. The information on this interface will refresh automatically

every 1 minute. You can manually refresh the interface at any time by right-clicking your mouse and selecting **Refresh** from the menu that appears.

The **Application Status Summary** table displays information about applications that you can access on local or remote networks via your company's secure application network:

Application — This field displays the name or type of application.

Status — This field displays the current status of the application. Possible statuses include:

Status	Description
Up	The application is currently active and can be used.
Down	The application is currently unavailable.
Unknown	This status may denote any of the following states: the application is down, the server is down, and/or there is no connectivity to the application or server.
Warning	If an application uses multiple protocols (for example, an email application would use both the POP protocol and the SMTP protocol), this status indicates that the test(s) for some of the protocol(s) are failing while others are succeeding OR the application has exceeded its warning threshold as defined by an administrator.
Critical	This status indicates that the application has exceeded its critical threshold as defined by an administrator.
N/A	A test used to determine the status of the application has not been configured in App Net Manager. Therefore, the status cannot be identified.

Last Status Change — This field displays the date and time that the application changed to its current status.

Comment — This field displays a short note written by the application's administrator.

Email — If it has been configured, an envelope icon will appear in this column that you can click to send an email message to the administrator of the application. This email link allows you to get in touch with the appropriate administrator for each application.

17.3.2 Administrator Interface

The **Administrator Interface** of **Monitoring** will be displayed if you have logged into Gateway Viewer via the **Admin Login** button and subscribed to the application monitoring and/or server monitoring service. This interface provides network administrators with tools for analysis and problem drill down concerning the network as well as the applications and servers running on the network. It is more complex than the user interface and contains multiple screens:

- Section 17.3.2.1, “Application Status on Network”
- Section 17.3.2.2, “Server Status on Network”
- Section 17.3.2.3, “Detailed Information on Application”

- Section 17.3.2.4, “Statistics History on Application”
- Section 17.3.2.5, “Detailed Information on Server”
- Section 17.3.2.6, “Statistics History on Server”
- Section 17.3.2.7, “Detailed Status on Application”
- Section 17.3.2.8, “Detailed Status on Server”
- Section 17.3.2.9, “Status History on Server”
- Section 17.3.2.10, “Update Comment”

You can set the refresh rate for the **Administrator Interface** of **Monitoring** by clicking the refresh icon that is displayed at the top of each page. Enter a value in the dialog box that appears. You can enter a value between 0 seconds and 3600 seconds (1 hour). This value is persistent and will be used for all **Monitoring** pages. The default refresh rate is 60 seconds (1 minute). A refresh rate of 0 seconds means that you do not want the page to automatically refresh. To manually refresh a page at any time, click the right mouse button within the frame that you would like to refresh and select the **Refresh** option from the menu that appears.

In general, do not use the **Back** button on your browser to navigate through the monitoring interface. This may cause cached information to be displayed. To ensure that you are viewing the most up-to-date data, use only the hyperlinks provided on the interface to load pages.

17.3.2.1 Application Status on Network

The **Application Status on Network** page provides a summary of the local applications, network links, and servers that are registered on the local Corente Services Gateway for monitoring and/or sharing with other application network locations. Selecting certain items on this page will display detailed information about those items. The tables that appear on this interface are determined by the services that you have subscribed to: if you have subscribed to application monitoring, the **Application Status Summary** table will appear, and if you have subscribed to server monitoring, the **Server Status Summary** table will appear. The tables on this interface can be sorted via any category simply by selecting that category's heading. The category that is currently used for sorting will be displayed in bold characters.

The **Network Statistics** table provides a summary of the traffic traveling to and through the local Corente Services Gateway. If the number of bytes recorded in any category exceeds 1024, the number of bytes will be rounded off and listed in K(ilobytes), M(egabytes), G(igabytes), etc.

Bytes on LAN	The total number of bytes, measured by the Corente Services Gateway, that have been sent on the LAN since the last time the Corente Services Gateway was started (i.e., the date/time in the **Network Statistics** section heading).
Bytes on WAN	The total number of bytes, measured by the Corente Services Gateway, that have been sent on the WAN since the last time the Corente Services Gateway was started (i.e., the date/time in the **Network Statistics** section heading). WAN traffic includes both Internet traffic and alternate connection traffic (i.e., non-secure-application network site-to-site traffic).
Bytes on App Network	The total number of bytes, measured by the Corente Services Gateway, that have been sent on the secure application network since the last time the Corente Services Gateway was started (i.e., the date/time in the **Network Statistics** section heading).

Bytes on LAN* — The total number of bytes, measured by the Corente Services Gateway, that have been sent on the LAN in the last 30-second interval. This 30-second interval is the 30 seconds preceding the last date and time the page was refreshed (i.e., the date and time displayed in the heading of this table).

Bytes on WAN* — The total number of bytes, measured by the Corente Services Gateway, that have been sent on the WAN in the last 30-second interval. WAN traffic includes both Internet traffic and alternate connection traffic (i.e., non-secure-application-network site-to-site traffic).

Bytes on App Network* — The total number of bytes, measured by the Corente Services Gateway, that have been sent on the secure application network in the last 30-second interval.

The **Application Status Summary** table displays a summary of information about each application that has been registered with the local Corente Services Gateway for use over the secure network.

Application — This field dispays the name or type of application. Click the entry in this field to display the Section 17.3.2.3, “Detailed Information on Application” page about this application. No hyperlink will be present if the application has only an ICMP protocol defined as no data is collected for such applications.

Status — This field displays the last reported status of the application. Click the entry in this field to display the Section 17.3.2.7, “Detailed Status on Application” page about this application's status. Possible entries in the field are:

Status	Description
Up	The application is currently active and can be used.
Down	The application is currently unavailable.
Unknown	This status may denote any of the following states: the application is down, the server is down, and/or there is no connectivity to the application or server.
Warning	If an application uses multiple protocols (for example, an email application would use both the POP protocol and the SMTP protocol), this status indicates that the test(s) for some of the protocol(s) are failing while others are succeeding OR the application has exceeded its warning threshold as defined by an administrator.
Critical	This status indicates that the application has exceeded its critical threshold as defined by an administrator.
N/A	A test used to determine the status of the application has not been configured in App Net Manager. Therefore, the status cannot be identified.

Last Status Change — This field displays the time that the application changed to its current status.

Comment

This field displays a short note about the application or its status that is displayed to users. Click the entry in this field to use the Section 17.3.2.10, “Update Comment” page to add a comment, delete the current comment, or change the current comment. This comment will be displayed on both the Section 17.3.1, “User Interface” and the Section 17.3.2, “Administrator Interface”.

17.3.2.2 Server Status on Network

The **Server Status on Network** table displays a summary of information about local servers that have been registered with the local Corente Services Gateway.

Server

This field displays the name or type of the server.

Status

This field displays the last reported status of the server. Click the entry in this field to display the Section 17.3.2.8, “Detailed Status on Server” page about this server's status. Possible entries in the field are:

Status	Description
Up	The server is currently active and can be used.
Down	The server is currently unavailable.
Unknown	This status may denote any of the following states: the application is down, the server is down, and/or there is no connectivity to the server.
Warning	If multiple resources are being monitored on the server (for example, the following resources can all be monitored--CPU Load, Disk Space Usage, Memory Usage, and Swap Space Usage), this status indicates that the test(s) for some of the resource(s) are failing while others are succeeding OR this status indicates that one or more of the resources have exceeded their warning thresholds, as defined in App Net Manager, and are generating a warning alarm.
Critical	This status indicates that one or more of the resources being monitored on the server have exceeded their critical thresholds, as defined in App Net Manager, and are generating a critical alarm.
N/A	A test used to determine the status of the server has not been configured in App Net Manager. Therefore, the status cannot be identified.

Last Status Change

This field displays the time that the server changed to its current status.

Comment

Because server monitoring data is viewable only by administrators, the comment field is unavailable.

17.3.2.3 Detailed Information on Application

The **Detailed Information on Application** page displays statistics and connection information about the application that you have selected.

The **Application Statistics*** table displays statistics from the last 30-second interval. This 30-second interval is the 5 seconds preceding the date and time that the page was last refreshed (i.e., the date and

time displayed at the bottom of the page). If the number of bytes recorded in a category on this table exceeds 1024, the number of bytes will be rounded off and listed in K(ilobytes), M(egabytes), G(igabytes), etc.

% of Traffic on LAN	The percent of the total traffic on the LAN during the 30-second interval that consisted of traffic to and from this application.
% of Traffic on WAN	The percent of the total traffic on the WAN during the 30-second interval that consisted of traffic to and from this application. WAN traffic includes both Internet traffic and alternate connection traffic (i.e., non-secure-application-network site-to-site traffic).
% of Traffic on App Network	The percent of the total traffic on the secure application network during the 30-second interval that consisted of traffic to and from this application.
Bytes from Application	The total number of bytes sent from the application to machines with active connections during the 30-second interval.
Bytes to Application	The total number of bytes sent to the application from machines with active connections during the 30-second interval.
Bytes Total	The total number of bytes both sent and received by this application during the 30-second interval.
# of Connections Added	The number of connections that were added during the 30-second interval.
# of Connections Dropped	The number of connections that were dropped during the 30-second interval.

The **Application Statistics** table displays host information, protocol, and traffic information about the selected application. If the number of bytes recorded in a category on this table exceeds 1024, the number of bytes will be rounded off and listed in K(ilobytes), M(egabytes), G(igabytes), etc.

Host Name	The name of server providing this application. Select the entry in this field to show the Section 17.3.2.5, “Detailed Information on Server” page for this server.
Host IP Address	The IP address of the server that is providing this application.
Service (Port)	The type of service/protocol and the corresponding port number that machines must use to make connections to this application. This field may contain multiple entries.
Duration (HH:MM:SS)	The amount of time between the date/time displayed in the heading of this section and the date/time displayed at the bottom of the page. The statistics within this section have all been collected during this duration.
Bytes from Application	The total number of bytes sent from the application to machines with active connections since the last time the Corente Services Gateway was last started (i.e., the date/time displayed in the heading of this section).
Bytes to Application	The total number of bytes sent to the application from machines with active connections since the last time the Corente Services Gateway was last started (i.e., the date/time displayed in the heading of this section).

Bytes Total	The total number of bytes both sent and received by this application since the last time the Corente Services Gateway was last started (i.e., the date/time displayed in the heading of this section).
# of Current Connections	The total number of current connections that are established to this application.

The **Connected Networks** table lists all of the networks with machines that are currently connected to this application. The total number of current connected networks is displayed in the title of the section. Click the **Show History** hyperlink to display the Section 17.3.2.4, "Statistics History on Application" page and view historical graphs of all active network connections to this application. If there are more than ten connected networks, an additional hyperlink will be displayed: click the **Top Ten** hyperlink to view historical graphs of only the top 10 network bandwidth users (based on the total number of bytes sent and received by the application to/from each network).

If the number of bytes recorded in a category on this table exceeds 1024, the number of bytes will be rounded off and listed in K(ilobytes), M(egabytes), G(igabytes), etc.

Network	The name of the Corente Services Gateway whose network has active connections with this application. If the Corente Services Gateway is within another domain and has an extranet connection with the local Corente Services Gateway, this entry will contain the Corente Services Gateway's full name (i.e., `domainname.gatewayname`). Note that the icon to the left of each entry in this column indicates whether the entry is a network or a remote Corente client .
Duration (HH:MM:SS)	The total duration of this network or remote client's connection to the application.
Bytes from App	The total number of bytes sent from the application to machines on this network or to this remote client since the last time the Corente Services Gateway was started (i.e., the date/time displayed in the heading of the **Application Statistics** section).
Bytes to App	The total number of bytes sent to the application from machines on this network or from this remote client since the last time the Corente Services Gateway was started (i.e., the date/time displayed in the heading of the Application Statistics section).
Bytes Total	The total number of bytes both sent and received by the application to and from machines on this network or this remote client since the last time the Corente Services Gateway was started (i.e., the date/time displayed in the heading of the Application Statistics section).
Bytes from App*	The total number of bytes sent from the application to machines on this network or to this remote client during the 30-second interval.
Bytes to App*	The total number of bytes sent to the application from machines on this network or from this remote client during the 30-second interval.
Bytes Total*	The total number of bytes both sent and received by the application to and from machines on this network or this remote client during the 30-second interval.

17.3.2.4 Statistics History on Application

The **Statistics History on Application** page displays graphs of the traffic (in bytes) sent and received by the application per 30-second interval from each network that is connected to the application. The

first graph details the traffic sent by the application, the second graph details the traffic received by the application, and the third graph details the total amount of traffic both sent by and received by the application.

Important

The data on this screen is captured as you view this screen and the application's **Detailed Information on Application** screen. If you move to another screen, the graphs may be reset to allow the Corente Services Gateway resources to be utilized more effectively. You must remain on these pages to collect the amount of historical data that you would like.

These graphs can provide up to 24 hours worth of information (the most recently captured data always appears on the right side of each graph). The total duration of the historical data that you have captured in the graphs is displayed in the heading of this page. As time passes, you will be able to view the graphs in shorter time increments (the last 10 minutes, the last 30 minutes, etc.) by using the links that also appear in the heading of this page. The graph increment that you are currently viewing is displayed in bold white characters.

If you modify the refresh rate on this page by selecting the refresh icon, you will not be able to set the refresh rate to intervals greater than every 10 minutes. If your refresh rate is already set to intervals greater than 10 minutes, it will automatically be changed to refresh every 10 minutes.

17.3.2.5 Detailed Information on Server

The **Detailed Information on Server** page displays statistics and connection information about the server that you have selected from a **Detailed Information on Application** page. A single server on your network can provide multiple applications via the Corente Services Gateway.

The **Server Statistics*** table displays statistics from the last 30 second interval. This 30-second interval is the 30 seconds preceding the date and time that the page was last refreshed (i.e., the date and time displayed at the bottom of the page). If the number of bytes recorded in a category on this table exceeds 1024, the number of bytes will be rounded off and listed in K(ilobytes), M(egabytes), G(igabytes), etc.

% of Traffic on LAN	The percent of the total traffic on the LAN during the 30-second interval that consisted of traffic to and from this server.
% of Traffic on WAN	The percent of the total traffic on the WAN during the 30-second interval that consisted of traffic to and from this server. The WAN includes Internet traffic and alternate connection traffic (i.e., non-secure-application-network site-to-site traffic).
% of Traffic on App Network	The percent of the total traffic on the secure application network during the 30-second interval that consisted of traffic to and from this server.
Bytes from Server	The total number of bytes sent from the server to machines with active connections during the 30-second interval.
Bytes to Server	The total number of bytes sent to the server from machines with active connections during the 30-second interval.
Bytes Total	The total number of bytes both sent and received by the server during the 30-second interval.
# of Connections Added	The number of connections that were added to this server during the 30-second interval.

# of Connections Dropped	The number of connections that were dropped from this server during the 30-second interval.

The **Server Statistics** table displays address and traffic information about the selected server. If the number of bytes recorded in a category on this table exceeds 1024, the number of bytes will be rounded off and listed in K(ilobytes), M(egabytes), G(igabytes), etc.

Host IP Address	The IP address of this server.
Duration (HH:MM:SS)	The amount of time between the date/time displayed in the heading of this section (the date/time that the server established its current UP status) and the date/time displayed at the bottom of the page (the date/time the page was last refreshed). The statistics within this section have all been collected during this duration.
# of Current Connections	The total number of connections that have been established to this server since the date/time displayed in the heading of this section.
Bytes from Server	The total number of bytes sent from the server to machines with active connections since the last time the Corente Services Gateway was started (i.e., the date/time displayed in the heading of this section).
Bytes to Server	The total number of bytes sent to the server from machines with active connections since the last time the Corente Services Gateway was started (i.e., the date/time displayed in the heading of this section).
Bytes Total	The total number of bytes both sent and received by this server since the last time the Corente Services Gateway was started (i.e., the date/time displayed in the heading of this section).

The **Connected Networks** table lists all of the networks with machines that are currently connected to this server. The total number of current connected networks is displayed in the title of the table. Click the **Show History** hyperlink to display the Section 17.3.2.6, “Statistics History on Server” page and view historical graphs of all active partner connections to this server. If there are more than ten connected networks, an additional hyperlink will be displayed: click the **Top Ten** hyperlink to view historical graphs of only the top 10 network bandwidth users (based on the total number of bytes sent and received by the server to/from each network).

If the number of bytes recorded in a category on this table exceeds 1024, the number of bytes will be rounded off and listed in K(ilobytes), M(egabytes), G(igabytes), etc.

Network	The name of the Corente Services Gateway whose network has active connections with this server. If the Corente Services Gateway is within another domain and has an extranet connection with the local Corente Services Gateway, this entry will contain the Corente Services Gateway's full name (i.e., domainname.gatewayname). Note that the icon to the left of each entry in this column indicates whether the entry is a network or a remote Corente client .
Duration (HH:MM:SS)	The total duration of this network or remote client's connection to the server.
Bytes from Srv	The total number of bytes sent from the server to machines on this network or to this remote client since the last time the Corente Services Gateway was started (i.e., the date/time displayed in the heading of the Server Statistics section).

Bytes to Srv	The total number of bytes sent to the server from the machines on this network or from this remote client since the last time the Corente Services Gateway was started (i.e., the date/time displayed in the heading of the Server Statistics section).
Bytes Total	The total number of bytes both sent and received the server to and from the machines on this network or remote client since the last time the Corente Services Gateway was started (i.e., the date/time displayed in the heading of the Server Statistics section).
Bytes from Srv *	The total number of bytes sent from the server to the machines on this network or to this remote client during the 30-second interval.
Bytes to Srv*	The total number of bytes sent to the server from the machines on this network or from this remote client during the 30-second interval.
Bytes Total*	The total number of bytes both sent and received by the server to and from the machines on this network or this remote client during the 30-second interval.

17.3.2.6 Statistics History on Server

The **Statistics History on Server** page displays graphs of the traffic (in bytes) sent and received by the server per 30-second interval from each network that is connected to the server. The first graph details the traffic sent by the server, the second graph details the traffic received by the server, and the third graph details the total amount of traffic both sent by and received by the server.

Important

The data on this screen is captured as you view this screen and the server's **Detailed Information on Server** screen. If you move to another screen, the graphs may be reset to allow the Corente Services Gateway resources to be utilized more effectively. You must remain on these pages to collect the amount of historical data that you would like.

These graphs can provide up to 24 hours worth of information (the most recently captured data always appears on the right side of each graph). The total duration of the historical data that you have captured in the graphs is displayed in the heading of this page. As time passes, you will be able to view the graphs in shorter time increments (the last 10 minutes, the last 30 minutes, etc.) by using the links that also appear in the heading of this page. The graph increment that you are currently viewing is displayed in bold white characters.

If you modify the refresh rate on this page by selecting the refresh icon, you will not be able to set the refresh rate to intervals greater than every 10 minutes. If your refresh rate is already set to intervals greater than 10 minutes, it will automatically be changed to refresh every 10 minutes.

17.3.2.7 Detailed Status on Application

The **Detailed Status on Application** page displays status information about the application that you have selected. The status of each protocol used by the application is presented in a separate table on this page.

The Application Information table displays identity information about the application being monitored.

Host Name	The DNS name of the server that is providing the application. If you are viewing the detailed status of an application, the entry in this field can

	be selected to display the Section 17.3.2.5, “Detailed Information on Server” page for this server.
Host IP Address	The IP address of the server that is providing the application.

The **Application Status** table displays the following information:

Service Protocol	The protocol used by machines to connect to this application. Each protocol employed by the application will have its own table on this page, with its own corresponding status information.
Service Port	The port number on the server used by machines to connect to the application with the **Service Protocol**.
Status	The summarized status of the **Service Protocol**.
Last Status Change	The date and time that the **Service Protocol** changed to its current **Status**.
Last Verification	The last date and time that the current status of the **Service Protocol** was verified.
Verification Interval	The period of time between automatic status verifications.
Verification Type	The type of test that the Corente Services Gateway will perform to verify the status of the **Service Protocol**. This test is chosen when registering the application/service with the Corente Services Gateway in App Net Manager.
Latency or Defective Samples	If the **Verification Type** is not **IP Network Quality**, then this field will be displayed as **Latency** and will indicate the average latency of **Service Protocol** packets sent to and from the application as determined by the verification test. If the **Verification Type** is **IP Network Quality**, this field will be displayed as **Defective Samples** and will indicate the percentage of defective traffic samples as determined by the **IP Network Quality** test. This test estimates network quality by measuring a combination of latency, jitter, and packet loss on traffic samples in an interval. Acceptability of a sample is determined by thresholds set by an administrator in App Net Manager.
Detailed Results	The detailed results of the verification test. The information provided in this field depends upon the **Verification Type** that has been configured for this **Service Protocol**. This field can be used to analyze and diagnose any problems with the application or its connection.

The **Verify Now** hyperlink at the top of each table can be used to verify the status of that table's **Service Protocol** immediately. This hyperlink can be used instead of waiting for the next automatic verification.

17.3.2.8 Detailed Status on Server

The **Detailed Status on Server** page displays usage information about resources on the server that you have selected.

The **Server Information** table displays identity information about the server being monitored.

Host Name	The DNS name of the server.

Host IP Address	The IP address of the server.
Show History	Click this hyperlink to display the Section 17.3.2.9, “Status History on Server” page for this server, which presents a historical graph of utilization for all resources that are being monitored on this page.

The **Server Status** table displays the following information for each resource that an administrator in App Net Manager has selected to be monitored on this server:

Resource Type	The resource whose status is displayed in this table. Possible resources are: CPU Load (in the last minute), Disk Space Usage, Memory Usage, and Swap Space Usage.
Usage Info	The percentage of this resource being used on the server.
Status	The summarized status of this resource on the server.
Last Status Change	The date and time that the resource on the server changed to its current **Status**.
Last Verification	The last date and time that the current status of the resource on the server was verified.
Verification Interval	The period of time between automatic status verifications.
Detailed Results	Additional information about the resource.

The **Verify Now** hyperlink at the top of each table can be used to verify the status of that resource immediately. This hyperlink can be used instead of waiting for the next automatic verification.

17.3.2.9 Status History on Server

The **Status History on Server** page displays a graph that details the percent utilization of resources that are being monitored for the server on the Section 17.3.2.8, “Detailed Status on Server” page. Usage of the following resources may be displayed on the graph: CPU, memory, swap space, and disk space. Usage of each resource is graphed using a different colored line.

Important

The data on this screen is captured as you view this screen. If you move to another screen, the graphs may be reset to allow the Corente Services Gateway's resources to be utilized more effectively. You must remain on these pages to collect the amount of historical data that you would like.

The graph can provide up to 24 hours worth of information (the most recently captured data always appears on the right side of the graph). The total duration of the historical data that you have captured is displayed in the heading of this page. As time passes, you will be able to view the graph in shorter time increments (the last 30 minutes, the last hour, etc.) by using the links that also appear in the heading of this page. The graph increment that you are currently viewing is displayed in bold white characters.

17.3.2.10 Update Comment

If you would like to provide users with information about an application or its status, you can add a comment to the users' **Monitoring** page by selecting the entry in that applications **Comments** field and entering information on this page.

Comment	Enter the comment in this field. You may use up to 50 characters.

Valid for	Select the period of time that this comment will be displayed on the **Monitoring** page. Enter a value in this field and select Minutes, Hours, Days, Months, or Years. When this period of time has expired, the comment will no longer be displayed.

When you have completed these fields, click the **Submit** button. If there is a current comment that has not yet expired for the application, that comment will be replaced by this new comment. To clear the fields and start again, click the **Reset** button.

17.3.3 Top Talkers

The **Top Talkers** page will be available from the **Monitoring** menu if you have logged into Gateway Viewer via the **Admin Login** button.

Top Talkers allows an administrator to monitor network activity between machines on the local network and machines at remote sites and/or the Internet, to identify what machine pairs are using up the most bandwidth (i.e., the "top talkers"). This feature is useful, for example, as a way of identifying machines infected by a Trojan horse or local users abusing BitTorrent.

When an administrator selects **Top Talkers**, the page will be opened using the default configuration settings. **Top Talkers** will begin after a 10 second delay, during which time it is gathering information. The **Top Talkers** page will then be updated automatically based on the refresh rate that you choose for the **Monitoring** pages. (The maximum refresh rate allowed for **Top Talkers** is 60 seconds. If a refresh rate longer than 60 seconds has been chosen for the **Monitoring** pages, the refresh rate will be temporarily changed while the **Top Talkers** page is open to refresh every 60 seconds. Similarly, the minimum refresh rate allowed is 10 seconds. If a refresh rate shorter than 10 seconds has been chosen, the refresh rate will be temporarily changed to 10 seconds while the **Top Talkers** page is open.) Each refresh presents new, non-aggregated data.

Only one administrator can monitor the **Top Talkers** page for a Corente Services Gateway at a time. If another administrator of the Corente Services Gateway attempts to open the **Top Talkers** page, an error message will be displayed to inform the administrator that someone else is already using it.

The page presents the following data in a table:

Local Host	The WINS name (if applicable) of the local machine in the top talker pair.
Local IP	The IP address of the local machine in the top talker pair.
Port	The port number being communicated with on the local machine in the top talker pair (when **Display Type** is **By Address and Port**; see Set Options).
Remote IP	The IP address of the remote machine to which the Local Host is "talking".
Remote Port	The port number being communicated with on the remote machine (when **Display Type** is **By Address and Port**; see Set Options).
Bytes Sent	The number of bytes sent by the local top talker to the remote machine.
Bytes Received	The number of packets or bytes received by the local top talker from the remote machine.
Bytes Total	The aggregate number of packets or bytes both sent and received by the local top talker to/from the remote machine.

An administrator can click **Set Options** to view or change the monitor and display options. Any new selections will apply to all subsequent reports until the options are changed again or you navigate to another page.

Note

Only the traffic that travels through the Corente Services Gateway will be measured by **Top Talkers**. This means that if your Corente Services Gateway is in the Peer configuration, only secure Corente Services network traffic and traffic that is specifically routed through the gateway will be included in the calculations.

Set Options

When you select **Set Options**, you can change how the **Top Talkers** page reports and displays data. You can change the options on this page as follows:

Interface	Select the network interface of the Corente Services Gateway that will be monitored for discovering top talkers. By default, the LAN-side interface of the gateway will be used.
Address Range	Enter an address pool of local IP addresses that will be included in calculating the top talkers. By default, this field will be filled in with the address range defined for that interface.
Display Type	Choose the way in which is data is examined and displayed. By default, **By Address and Port** will be selected. Bandwidth use will be examined in port number to port number pairs between each pair of local and remote machines. This can be helpful for administrators, if they are trying to narrow down the specific bandwidth stealing culprits on the machine pairs (i.e., web traffic, a specific application, etc.). Selecting **By Address Only** will change **Top Talkers** monitoring so that top talkers will be determined by the total traffic between machine pairs.
Duration	Enter the amount of time (in seconds) for monitoring. By default, the duration is set to 10 seconds.
Report Count	Enter the number of top talkers to display. By default, the top 10 talkers will be displayed. The maximum number of top talkers that can be displayed is 50.

When you select Submit to save your changes, the new options will apply to all subsequent **Top Talkers** refreshes (until the options are changed again). If you navigate to another page, all options you have changed will return to the default values.

17.4 Networks

The options available in the **Networks** menu allow you to browse computers on your secure application network just as you would use **Network Neighborhood** to browse computers on your local network. While **Network Neighborhood** only provides access to Windows PCs, the **Network Neighborhood** allows you to browse even the non-Windows computers that participate in your secure network.

The following options are available in the **Networks** menu:

- Section 17.4.1, “Local Network” allows you to browse all computers on your local Corente Services Gateway network.

- Section 17.4.2, “Remote Networks” allows you to browse remote Corente Services Gateways and computers on the secure network.

17.4.1 Local Network

Computers on your local network are listed on this page alphabetically. A machine whose name is not known, e.g., it does not register in the Domain Name System (DNS), will be listed by its IP address. Windows computers that are not configured as either file or print servers will not be listed.

- When using Internet Explorer, if a machine is configured as an SMB-based file/printer server, there will be a hyperlink available for that machine. You can simply click the link to browse the shared resources on that server or place your cursor over the link to view the server's IP address. Computers with hyperlinks will be listed before the computers without hyperlinks. Non-Windows computers that do not have file/print services running on the system will be listed without hyperlinks. Although you will not be able to access these computers directly from this interface, you can use any other protocols to connect to these machines, e.g, FTP, HTTP, telnet, etc.
- When using Firefox or Safari, no hyperlinks will be displayed as these web browsers do not support file browsing. Although you will not be able to access computers and file servers directly from this interface, you can use any other protocols to connect to these machines, e.g, FTP, HTTP, telnet, etc.

Computers that have been disconnected from the network will be removed from the local computer list within 30~45 minutes. You can click **Local Network** again or right-click your mouse button within the bottom frame of the page and select the **Refresh** option from the menu that appears to view the most up-to-date list. If you do not manually refresh the page, the page will automatically update every 15 minutes.

Note

- The computer that you are currently using will be highlighted in gray.
- You can connect to computers on the local network even when the Corente Services Gateway is not running.
- If you are using Internet Explorer 9.0 or later, in order to be able to browse the shared resources on a server, you need to add the Gateway Viewer URL to the **Trusted Sites** zone.

17.4.2 Remote Networks

This interface allows you to browse your Location Partners within the secure application network and all computers on each remote network.

Note

- Your computer needs the proper Corente Services Gateway access permissions in order to connect to Location Partners and computers on the secure network. Only Corente Services Gateways and computers that you are allowed to access from your computer will be listed in **Remote Networks**.
- You can connect to computers on remote networks only when the Corente Services Gateway software is running.

Connect to Computers on Remote Networks

The **Connect to computers on Remote Networks** page displays all remote Corente Services Gateway that you are allowed to access and that are currently up and running. Click on a Corente Services Gateway to browse computers within that remote Corente Services Gateway network.

If you have access to any Corente Services Gateways from another company's secure application network, they will be listed on this page by their full Corente Services Gateway name, i.e., `domainname.gatewayname`.

Remote Corente Services Gateways that have disconnected from the secure network will be removed from this page immediately. You can click **Remote Networks** or right-click your mouse button within the bottom frame of the page and select the Refresh option from the menu that appears to view the most up-to-date listing of Corente Services Gateways. If you do not manually refresh the page, the page will automatically update every 15 minutes.

Connect to Computers on Each Remote Network

The **Connect to computers on remote network** page displays the computers on the remote Corente Services Gateway network that you have selected. This page is very similar to the Connect to machines on **Local Network** page; you can refer to that section of the help document for additional browsing information.

If you are using Internet Explorer, you can place your cursor over a hyperlink to view a remote computer's IP address. When you click on a link for a specific computer, your machine will be connecting to the remote machine with this IP address. This IP address may be translated (i.e., it may be different than the real IP address of the remote computer).

To display both the connection IP address and the real IP address of the computers on the remote network, click on the **Show All** link available at the top of the computer list box. To display the connection IP address only (default), click on the **Show One** link.

You can use the computer names that are listed on this page for all network connections, such as map network drive, FTP, HTTP, telnet, etc. You can access a remote machine by name even if you do not have any name services configured on your computer (e.g., WINS or DNS).

Remote computers that have been disconnected from the secure network will be removed from the remote computer list within 30~45 minutes. You can right-click your mouse button within the bottom frame of the page and select the Refresh option from the menu that appears to view the most up-to-date computer listing for a particular network. If you do not manually refresh the page, the page will automatically update every 15 minutes.

Note

- If you receive a message that `The page cannot be displayed` after you click on the link of a remote computer, try right-clicking your mouse button within the bottom frame of the page and select the **Refresh** option from the menu that appears to update the current page. Sometimes the responses from the server will not be displayed correctly until you refresh the page.

  Just like accessing servers within your local network, you need the proper file/print sharing permissions to browse and access the resources on a remote server. Usually the authentication is based on the user name/password that you use to log on to your local computer.

  If a computer is disconnected from the network, it may still be listed on this page for 30~45 minutes. If you try to connect to the computer during this period of time, you will receive an error message.

- You can connect to computers on the remote network only when the Corente Services Gateway software is running.

- If you are using Internet Explorer 9.0 or later, in order to be able to browse the shared resources on a server, you need to add the Gateway Viewer URL to the **Trusted Sites** zone.

17.5 Network Admin

The options available in the **Network Admin** menu allow you to monitor and control the connections that this Corente Services Gateway provides. The options in this menu are intended for use by administrators only.

When you attempt to access an option from the **Network Admin** menu, a dialog box may appear that requests a user name and password. Enter these items and click **OK**. You will only be asked for this information once per administration session. Your user name and password will be saved until you close your browser window.

- Section 17.5.1, “NAT Info” allows you to view the **Outbound NAT** and **Auto Resolve/Inbound NAT** information for the IP addresses on the network.
- Section 17.5.2, “Monitor Computer” allows you to select what type of computers will be updated in the list on the **Local Network** page.
- Section 17.5.3, “Add Computer” allows you to add one or more computers to the local Corente Services Gateway network.
- Section 17.5.4, “Remove Computer” allows you to delete computer(s) from the local Corente Services Gateway network.
- Section 17.5.5, “Mobile User Report” allows you to view the mobile users currently connected to the local Corente Services Gateway.

17.5.1 NAT Info

The **Gateway NAT** information page displays information about the IP addresses that the local Corente Services Gateway is using for Network Address Translation (NAT). When connecting locations for your secure application network, overlapping IP addresses will create a problem. If two networks in different locations contain IP addresses in the same address space, packets will not get routed to the appropriate computers. NAT is often used to solve this problem.

This page allows you to check the NAT settings for the local Corente Services Gateway and determine what addresses the Corente Services Gateway is using to NAT each local or remote subnet, according to how NAT has been enabled for this Corente Services Gateway in the App Net Manager application.

The information is divided into categories for each NAT option: **Outbound NAT** and **Auto Resolve/ Inbound NAT**.

Outbound NAT

Outbound NAT is enabled on the local Corente Services Gateway for local subnets that are participating in the secure network. A network administrator identifies a local subnet that the Corente Services Gateway will NAT to another subnet before the subnet is made visible to remote Location Partners. The administrator is able to specify the subnet that will be used for NATing.

- The **User Group** column lists the real IP addresses and netmasks of all local subnets that are participating in the secure network.

- If Outbound NAT has been specified for a local subnet, the **NAT** column will display the NATed IP address of that subnet. (This is the subnet of IP addresses that Location Partners will use to make connections to the machines.) If Outbound NAT has not been enabled for this subnet, the column will display "N/A" and Location Partners will use the real IP addresses of the machines for secure connections.

If there are any Corente Clients that connect to this Location, any subnets that are being NATed by Outbound NAT will be listed twice. One entry will list the subnet as NATed, the other entry will not. This occurs because NAT does not function between Corente Client Partners and their host Corente Services Gateway. Corente Clients connect to the Corente Services Gateway like local clients rather than remote partners, so they connect to servers using real IP addresses.

To facilitate data viewing, you can sort the entries in this table by **User Group** subnet or by NAT subnet simply by clicking on the headings at the top of each column. The entries will be sorted in order, from lowest to highest subnet.

Auto Resolve/Inbound NAT

Auto Resolve/Inbound NAT are enabled on the local Corente Services Gateway for each partner. **Inbound NAT** will re-map all IP addresses in the partner's User Group to a new set of addresses that have been chosen by a network administrator, while **Auto Resolve NAT** will automatically perform NAT if a conflict is detected between the User Group of the local Corente Services Gateway and the User Group of the partner. If an IP address conflict is detected when Auto Resolve is enabled, the local Corente Services Gateway will NAT the partner's subnets to a new subnet (chosen by the Corente Services Gateway) so that local machines will be able to access computers in the partner's User Group. Both types of NATing will only occur locally; the NAT will be invisible to the remote computers.

- The **Partner** column lists the fully-qualified name of the partner (e.g., `domainname.gatewayname`) that is participating in NAT with the local Corente Services Gateway.

  The **User Group** column lists the real IP addresses and netmasks of the subnets of this Location Partner. (Depending upon what is included in the Location Partner's User Group, there may be multiple subnets per partner.)

- The **NAT** column will display the NATed IP addresses of these subnets. Local computers will use these translated IP addresses for secure network connections.

Auto Resolve NAT partners will not be listed unless Auto Resolve NAT is currently occurring with this partner. In order for Auto Resolve NAT to solve addressing conflicts between two partners, it must be enabled on both sides of the connection (i.e., both the local Location and the Location Partner must enable **Auto Resolve** for each other).

To facilitate data viewing, you can sort the entries in this table by **Partner**, **User Group** subnet, or by **NAT** subnet simply by clicking on

	the headings at the top of each column. The entries will be sorted in order, either alphabetical (for **Partner** entries) or from lowest to highest subnet (for **User Group** or **NAT** entries).

17.5.2 Monitor Computer

The **Monitor Computers on the Local Corente Gateway Network** page allows you to select what type of computers will be automatically listed and updated on the Local Networks page.

When a computer connects and disconnects from the secure application network, it is automatically removed or added to the **Local Network** page. It is also automatically removed or added to the **Remote Networks** page of any partners with the proper permissions to access that computer. By default, all computers on the local network (both Windows and non-Windows) are automatically monitored, and therefore automatically added or removed from the lists.

However, you may want the Corente Services Gateway to monitor only Windows computers if you are concerned about extra traffic on the local network, as non-Windows computers are monitored via periodic query requests from the Corente Services Gateway. Windows computers, however, are monitored via the announcements to the LAN from these computers. This does not generate any additional traffic on the local network.

Monitor all computers on local network	Select this option to monitor all computers on the local network. (This option is selected by default.)
Monitor only Windows computers on local network	Select this option if you do not want the non-Windows computers to be automatically monitored.

Any change to the **Monitor Computer** option takes effect immediately. If you select **Monitor only Windows computers** and click the **Submit** button, all non-Windows computers will be deleted immediately from the **Local Network** page and the **Remote Networks** pages of partners. If you later decide to select **Monitor all computers** again, all non-Windows computers that the Corente Services Gateway can detect will be re-added to the pages immediately.

Note

- If you have selected **Monitor only Windows computers**, yet users also need to access certain non-Windows computers, you can manually add these non-Windows computers to the **Local Network** page using the **Add Computer** option.
- You can change the **Monitor Computer** option only when the Corente Services Gateway software is running.

17.5.3 Add Computer

The **Add Computers to the Local Corente Gateway Network** page enables you to add any computers on the local network to the secure application network. However, there should be no need to use the **Add Computer** interface to add any machines to the local Corente Services Gateway network.

- If there is a Windows machine and you would like other users on the secure network to view that computer, you should simply install the File and Printer Sharing for Microsoft Networks component on that system. As long as a Windows PC is running file/print services, it will be added to the local Corente Services Gateway network automatically.
- Computers that are on the same subnet as the Corente Services Gateway are automatically added to the local network (including those computers that provide file/print services as well as non-Windows

computers). Windows computers that are on a different subnet than the local Corente Services Gateway can also be automatically added if the router of that subnet can be configured to forward the UDP broadcast packets within its network to the Corente Services Gateway.

If you are unable to re-configure a computer and/or a subnet so that the computer(s) will be automatically added to the network, you can manually add that machine with the **Add Computer** option. You can specify both the name and the IP address of the machine to be added. Both name and IP must be unique within the local network in order for the machine to be added successfully.

A computer that is manually added with this option will be listed on the **Local Networks** page. It will be listed with a hyperlink when Gateway Viewer is accessed with Internet Explorer; you can simply click the link to browse the shared resources on that server or place your cursor over the link to view the server's IP address.

A manually-added machine will be persistent, i.e., it will never be deleted automatically and can only be removed by using the **Remove Computer** option. If a machine is added manually, it will not be updated dynamically.

Remember that appropriate Corente Services Gateway access permissions (i.e., User Groups and/or shared applications) are needed so that the appropriate computers on the local Corente Services Gateway network will appear automatically on the **Remote Networks** pages of other networks within the secure network.

Note

- You will receive an error message if you try to add a computer when it has already been added to the network.
- You can add a computer to the local network only when the Corente Services Gateway software is running.

17.5.4 Remove Computer

The **Remove Computers From the Local Corente Gateway Network** page displays computers on the local Corente Services Gateway network and allows you to remove those computers that should no longer be accessible on the secure application network.

Note

This option should be used to remove only local computers that have been added with the **Add Computer** tool. All other local computers are automatically added and removed from Gateway Viewer as they are added and removed from the physical network. To prevent a computer that was not added with the **Add Computer** tool from being listed in a partner's Gateway Viewer, you must modify the User Groups of this Corente Services Gateway in the App Net Manager application and remove the computer's IP address from the Default User Group.

This interface can be used to remove computers that normally are added and removed automatically only if these computers have disconnected from the network and Gateway Viewer has not yet registered this information (as computers can take 30-45 minutes to be removed automatically from the **Local Networks** page). If you remove this type of computer when it is not disconnected, be aware that it will be re-added to the interface.

To remove a computer on this interface, simply check the computer and click the **Submit** button. There is no limitation on how many computers can be deleted at once.

Note

- If a computer has been added using the **Add Computer** button, it will never be deleted automatically from the **Local Network** or **Remote Networks** pages, even when it disconnects from the network or is shut down. You must use this interface to remove such computers from the secure network.
- The computer that you are currently using will be highlighted in gray.
- You can remove computers from the local network only when the Corente Services Gateway software is running.

17.5.5 Mobile User Report

The **Corente Gateway Mobile User Report** in Gateway Viewer allows an administrator to view which Mobile Users are currently connected to the Corente Services Gateway.

- **Time** displays the time when the Mobile User first connected.
- **User ID** displays the Mobile User name of the device.
- **Network Interface** displays the network interface of the Corente Services Gateway to which the Mobile User is connected.
- **IP Address** displays the IP address that was assigned to the Mobile User when they connected to the Corente Services Gateway.
- **Log History** lets you view a history of Mobile User connections to the Corente Services Gateway.

Log History

The **Log History** page displays a historical record of Mobile User connections to the Corente Services Gateway.

- **Time** displays the time when the Mobile User first connected.
- **User ID** displays the Mobile User name of the device.
- **Duration** displays the duration of the connection.
- **Bytes Sent** displays the number of bytes sent by the Mobile User to the Corente Services Gateway.
- **Bytes Received** displays the number of bytes received by the Mobile User from the Corente Services Gateway.

17.6 Gateway Admin

The options available in the **Gateway Admin** menu allow you to monitor and control the local Corente Services Gateway. The options in this menu are intended for use by administrators only.

When you attempt to access an option from the **Gateway Admin** menu, a dialog box may appear that requests a user name and password. Enter these items and click **OK**. You will only be asked for this information once per administration session. Your user name and password will be saved until you close your browser window.

The following options are be available from this menu:

- Section 17.6.1, “Status” displays the name of the Corente Services Gateway, IP address information (LAN, WAN, and VIP), current time, uptime, load averages, and Corente Services Gateway software

version information, as well as current information about the tunnel connections associated with this Corente Services Gateway.

- Section 17.6.2, “Test” allows you to perform several network connectivity tests to verify the operational status of the Corente Services Gateway, the Corente SCP, your DNS server, and the partners of the Corente Services Gateway.
- Section 17.6.3, “Control” allows you to start/stop/restart the Corente Services Gateway software and shutdown/reboot the Corente Services Gateway.
- Section 17.6.4, “Remote Login” allows you to select whether or not to allow remote login access to this Corente Services Gateway over the secure tunnel from the Corente Services Control Point.
- Section 17.6.5, “Download” allows you to download the Corente Services Gateway log files into a single compressed file that can be sent to Customer Care for troubleshooting purposes. You can also download a text file for each of the SNMP MIB files that are available on the Corente Services Gateway to review the information that each MIB can provide.
- Section 17.6.6, “Version” allows you to view version information about software that is installed on your Corente Services Gateway.

Note

Occasionally, you may see an image at the top of your **Gateway Administration** screens that indicates that your Corente Services Gateway has downloaded an upgrade of the Corente Services Gateway software, but must reboot in order to enable it. Clicking on the notification will take you to the **Control** screen, which you should use to manually reboot the Corente Services Gateway.

This notification will appear only if your Corente Services Gateway does not automatically reboot when an upgrade has been downloaded. To enable the automatic reboot so that upgrades will automatically go into effect, an administrator of your Corente Services Gateway can use the App Net Manager application to select **Allow automatic reboot after maintenance** on the **Location** tab of the Location form for your Corente Services Gateway.

17.6.1 Status

The **Corente Gateway Identity and Connection Status** page is divided into two sections: **Corente Gateway Information** and **Connection Status**. In addition, a **Show Detail** hyperlink appears at the top of the page. When clicked, this hyperlink provides additional information in the **Connection Status** section.

This page does not auto-refresh. When you want to view the most up-to-date information, right-click your mouse button over the interface and select the **Refresh** option from the menu that appears.

Corente Gateway Information

The first section of the **Status** page presents the following information about the Corente Services Gateway that you are viewing:

Name	Displays the name that was assigned to this Corente Services Gateway when it was created with the App Net Manager. This name is also used as the hostname for the Corente Services Gateway. The name will occasionally be prefixed with the name of your secure application network domain to generate a fully-qualified and unique Corente Services Gateway name (for example, domainname.gatewayname).
LAN Address	Displays the IP address assigned to the LAN (Local Area Network) Ethernet interface of the Corente Services Gateway. If the Corente

Services Gateway uses a **Peer** configuration, there is only one Ethernet interface, and its address will be listed in this field. If the Corente Services Gateway uses an **Inline** configuration, there are at least two Ethernet interfaces. The **LAN Address** will be the Ethernet interface that connects to the private internal network.

WAN Address

Displays the IP address assigned to the WAN (Wide Area Network) Ethernet interface of an Inline Corente Services Gateway. This interface connects to the public (Internet facing) network. A Peer configuration does not have a WAN interface. If the Dual WAN feature has been enabled, this is the address assigned to the primary WAN interface and is currently in use only when the word **ACTIVE** appears next to this entry.

Secondary WAN Address

Displays the IP address assigned to the secondary WAN (Wide Area Network) Ethernet interface of an Inline Corente Services Gateway, when the Dual WAN feature has been enabled. This secondary interface connects to the public (Internet facing) network and is currently in use only if the word **ACTIVE** appears next to this entry.

DMZ Address

Displays the IP address assigned to the DMZ-facing Ethernet interface of a Corente Services Gateway. Using this interface, the Corente Services Gateway acts as an intermediary between servers on the DMZ and those machines (both on the LAN and on the Internet/WAN) who access the servers. This arrangement prevents unwanted Internet/WAN traffic from infiltrating the LAN.

Virtual IP Address

Displays the internal IP address that was assigned when this Corente Services Gateway was created. A VIP address will be assigned for both **Peer** and **Inline** Corente Services Gateway configurations. This address is used for internal routing purposes when secure tunnels are being created. You cannot use this address for any other machine in your network, and you cannot communicate with the Corente Services Gateway via this address using programs such as telnet or ping.

LAN DHCP

Displays the status of DHCP on the LAN interface. The values in this field reflect the settings on the **Network** tab of the **Location** form for this Corente Services Gateway in App Net Manager. Values are as follows:

Status	Description
N/A	This field does not apply to this Corente Services Gateway.
none	This interface does not support DHCP.
client	This Corente Services Gateway receives its network configuration via a DHCP server.
server	This Corente Services Gateway is a DHCP server for computers on its subnet.

WAN DHCP

Displays the status of DHCP on the WAN interface. The values in this field reflect the settings on the **Network** tab of the **Location** form for this Corente Services Gateway in App Net Manager. Values are as follows:

Status	Description
N/A	This field does not apply to this Corente Services Gateway.
none	This interface does not support DHCP.
client	This Corente Services Gateway receives its network configuration via a DHCP server.
server	This Corente Services Gateway is a DHCP server for computers on its subnet.

Secondary WAN DHCP

Displays the status of DHCP on the secondary WAN interface. The values in this field reflect the settings on the **Network** tab of the **Location** form for this Corente Services Gateway in App Net Manager. Values are as follows:

Status	Description
N/A	This field does not apply to this Corente Services Gateway.
none	This interface does not support DHCP.
client	This Corente Services Gateway receives its network configuration via a DHCP server.
server	This Corente Services Gateway is a DHCP server for computers on its subnet.

Time

Displays the current time on the Corente Services Gateway from the operating system clock.

Uptime

Displays the amount of time since the Corente Services Gateway was last stopped.

Load

Displays the CPU utilization load average on the Corente Services Gateway (three averages are displayed - 1 minute average, 5 minute average, and 15 minute average, respectively).

Active Software

Indicates the version of the Corente Services Gateway software stored on the boot partition and currently active on the Corente Services Gateway. The Corente Services Gateway stores two versions of the Corente Services Gateway software - the currently active version (the version that was used at the last system boot) and the inactive version. The state of the software is indicated in the parentheses.

Possible states are listed in the following table: Table 17.1, “States for Active Software and Other Software”.

Other Software

Indicates the version of the Corente Services Gateway software stored on the special non-boot partition of the Corente Services Gateway (/clone). The inactive version could be an earlier or later version relative to the currently active version. It may be the last release to work on this Corente Services Gateway (in case the currently active software fails), or it may be the most recent upgrade of the software waiting to be activated when the Corente Services Gateway reboots. The state of the software is indicated in the parentheses.

	Possible states are listed in the following table: Table 17.1, “States for Active Software and Other Software”.
Hardware Failover	Indicates whether or not hardware failover (also known as redundant hardware) has been enabled on this Corente Services Gateway. If hardware failover is enabled, a number (1 or 2) will appear next to this field to identify the Corente Services Gateway hardware that is currently active.

The possible states for both **Active Software** and **Other Software** are as follows:

Table 17.1 States for Active Software and Other Software

State	Description
INITIAL	This is the first time Corente Services Gateway software has run on this machine.
UNKNOWN	The state of this software is unknown and should not be switched to. This is typically the result of a failed upgrade.
STAGING	The partition is in the process of staging an upgrade to a new version of the software and should not be switched to.
STAGED	A new version of the software has finished STAGING and is ready to be ARMED.
ARMED	The partition is set as ready to run on the next reboot.
BOOTING	A new release is running for the first time, but has not yet created a tunnel to the Corente Services Control Point (SCP). If failure occurs in this state, the active software will automatically switch to what is stored on the /clone partition (which should contain the last working release).
WORKS	The release works (or has worked at least once - enough to create a secure tunnel to the Corente SCP).
FAILED	If a new release fails to contact the Corente SCP after a specified amount of time, the release is marked FAILED and an automatic return to the /clone partition (which should contain the last working release) is initiated.

Connection Status

The bottom section of the **Status** page presents information about the status of all secure tunnels associated with this Corente Services Gateway. There are two types of tunnel connections displayed here:

- The **SCP Connection** is a connection that every Corente Services Gateway creates with the Corente Services Control Point (SCP). This secure tunnel is used whenever you administer your secure network with the App Net Manager.
- **Gateway to Gateway Connections** are the connections between your Corente Services Gateway and each of its remote Location Partners. These connections will be listed by the name of each remote Corente Services Gateway (for example, `domainname.gatewayname`).

The type of Transport (or protocol) that is used for each connection will be listed beside the connection name, as follows:

- **TCP** indicates the connection uses Transmission Control Protocol (TCP).

- **UDP** indicates the connection uses User Datagram Protocol (UDP).
- **NATIVE** indicates the connection belongs to a third party device.

In addition to the **Transport** type, the **Connection** and **Security** state of each connection will also be listed.

The meanings for each possible connection and security state are presented in the following tables:

Connection State	Description
Unknown	The connection is in the process of being established.
Established	The connection is fully established.

Security State	Description
Inactive	The Corente Services Gateway is waiting for contact from this partner. No tunnel connection will be established until this partner replies to the Corente Services Gateway.
In Progress	The secure tunnel is in the process of being established.
Secure	The tunnel is secure.
Terminating	The tunnel is being torn down.
Configuration Alert	This Corente Services Gateway and its partner are able to communicate with each other; however, the User Group(s) that each partner is exporting to the other contain conflicting address spaces. You must use one of the NAT options on the User Group or Partners tabs of the Location form in App Net Manager to remap one of the User Groups to a new address space or manually reconfigure one of the conflicting subnets to resolve this alert.

A **Show Detail** hyperlink is available at the top of the page. This detailed view gives more information about the status of the Corente Services Gateway's Ethernet interfaces and each connection between the Corente Services Gateway and its partners. This information is typically used only by technical support personnel.

The **Corente Gateway Interface Details** section lists eight possible Ethernet interfaces and describes the status of each interface's current links. For Peer Corente Services Gateways, eth0 functions the WAN/LAN interface. For Inline Corente Services Gateways, eth0 and eth1 function as the WAN and LAN interfaces. If WIFI is being used, an additional Ethernet interface will be listed with its current status. If an Ethernet interface is not in use, it will be listed as "Unavailable".

The information displayed in the **Connection Status** table when **Show Detail** is clicked includes:

Detail	Description
Name/(Transport)	The name of the Location Partner and the protocol used for the connection (either TCP or UDP). If a connection has not been established, the **Transport** will be listed as **Unknown**.
IP/VIP Address	The visible IP address of each Location Partner and the Virtual IP address assigned to this partner by the Corente SCP.
Latency (msec)	Latency over the secure connection to the Location Partner, in msec.
Conn/Security State	The state of the TCP/UDP connection and the state of the IPSEC connection.

You can return to the summarized **Connection Status** information by clicking on **Show Summary**.

17.6.2 Test

The **Test Network Connectivity** page provides a method for testing connectivity between the Corente Services Gateway and its partners, your DNS servers, the Internet, and the Corente Services Control Point (SCP).

Network Tools

This table provides several tools that allow you to test connectivity and network performance:

Test SCP Connectivity	To test connectivity from this Corente Services Gateway to the Corente SCP, click the **Test SCP Connectivity** button. On the page that is displayed, click **Test Network** to begin the test. When this test is successful, the network setup of the Corente Services Gateway (including all IP address, network mask, and default Internet gateway information, as well as the associated physical wiring) has been validated. The Corente Services Gateway's ability to communicate with the Corente SCP over a secure tunnel via the Internet has also been validated. If the test does not succeed, failure codes will be returned to help debug the problem.	
Packet Capture	This button allows you to perform packet traces through the Corente Services Gateway. When you click this button, the **Packet Capture** page will be displayed.	
	Interface	Select the interface of the Corente Services Gateway through which the packets will be traced and then displayed to you as a log. You can select one of the following: • **Any** for any available interface. • **WAN/LAN** interface if you are using a **Peer** configuration. • **WAN** interface or **LAN** interface if you are using an **Inline** configuration. • **GRE** interface if a GRE tunnel is configured for the LAN. • **DMZ** interface if a DMZ interface is configured on this Corente Services Gateway.
	Host IP or Name	If you would like, you can specify the host name or IP address of entities to isolate in your packet capture and only capture packets that travel between them and the Corente Services Gateway. You may enter one or more entries in this field, but you MUST separate the entries using

	either the and or the or modifier. This field is optional.
Operator	Select a modifier to define how to combine the entrie(s) in the **Host IP or Name** field with the entrie(s) in the **Service Port or Name** field when performing the packet capture. Selecting and will capture only packets that meet the criteria in both fields, while selecting or will ensure that packets need only meet the criteria in one of the fields to be captured.
Service Port or Name	If you would like, you can specify the service port or port name to isolate in your packet capture and only capture packets that travel to and from that port on the Corente Services Gateway.You may enter one or more entries in this field, but you MUST separate the entries using either the and or the or modifier. This field is optional.
Duration	Enter the duration (in seconds) for which you would like the packet capture to be performed. You may enter between 1 and 120 seconds. The default is 20 seconds.
	After you make your selections and fill out the fields, click the **Submit** button to perform the packet capture. The Processing page will be displayed while the packets are being captured. You may interrupt the capture at any time by clicking the **Stop and View** button on this page to see what packets have been captured up until that point. When the packet capture has completed or has been interrupted, you can click the **Save Capture** button at the bottom of the log to save the packet capture log to your computer as a `.txt` file. If the **Save Capture** button is not displayed, you can save the log by right-clicking the page and selecting **Select All** from the menu that appears, then right-clicking the highlighted text and selecting **Copy**.

	Then you can paste the text in a text editor and save the file.
Host	Lets you specify an IP address or DNS name of any computer that is accessible by this Corente Services Gateway. You can then either ping the computer or perform a traceroute.
Ping	Ping is a computer network tool used to test whether a particular host is reachable across an IP network. Enter an IP address or DNS name that you would like this Corente Services Gateway to ping in the **Host** field and click the **Ping** button.
Traceroute	Traceroute is a networking tool used to determine the route taken by packets across an IP network. The results of the test you select will be displayed on a new page in Gateway Viewer. Enter an IP address or DNS name to which you would like this Corente Services Gateway to traceroute in the **Host** field and click the **Traceroute** button.
Mtr	MTR combines the functionality of ping and traceroute into a single network diagnostic tool. It probes routers on the route path by limiting the number of hops individual packets may traverse, listening to responses of their expiry. It will regularly repeat this process and keep track of the response times of the hops along the path. Enter an IP address or DNS name to which you would like this Corente Services Gateway to MTR in the **Host** field and click the **Mtr** button. This report will cycle five (5) times (i.e., send five pings).

Network Interface

This table lists each Ethernet interface of the Corente Services Gateway and their statuses:

Name	The name of the interface. (LOOPBACK is the standard IP address used for a loopback network connection.)
Status	The status of the interface.
IP Address	The IP address currently assigned to the Ethernet interface.
Ping	Whether or not the Corente Services Gateway can successfully ping this interface. This entry should read Echo.
Default Gateway	The IP address of the default Internet gateway for this interface. Only **WAN** or **WAN/LAN** interfaces will have a **Default Gateway**.
Ping	Whether or not the **WAN** or **WAN/LAN** Ethernet inteface can successfully ping the **Default Gateway**.

Domain Name Server

This table lists each Domain Name Server (DNS) Server that is registered on this Corente Services Gateway:

DNS	Whether the DNS server is the **Primary** or the **Secondary** server.
IP Address	The IP address assigned to the DNS server.
Ping	Whether or not the **LAN** or **WAN/LAN** Ethernet interface of this Corente Services Gateway was able to successfully ping this DNS server when the **Test** page was loaded.

Test	Click the **Ping** button to ping the IP address of this DNS server, the **Traceroute** button to traceroute to the IP address of this DNS Server, or the **Mtr** button to MTR to the IP address of this DNS Server.

DNS Query

If this Location is configured as a DNS Server or DNS Updater, the **Test** page will include this table. When you click on the **Query** button in this table, the answers from all DNS servers that respond to the query will be displayed. This includes all of the DNS entries within the DNS zone that this Corente Services Gateway serves, and entries for the subzones of this zone (that provide the name of the subzone and either the VIP address of the Corente Services Gateway or the IP address of the third-party DNS server in charge of this subzone).

Internet

This table displays the following information about the Corente SCP:

Name	The name of the Corente SCP.
IP Address	The IP address assigned to the Corente SCP.
Ping	If the **WAN** or **WAN/LAN** Ethernet interface of the Corente Services Gateway can successfully ping the Corente SCP.
Test	Click the **Ping** button to ping the IP address of this entity, the **Traceroute** button to traceroute to the IP address of this entity, or the **Mtr** button to MTR to the IP address of this entity. The results of the test that you select will be displayed on a new page in Gateway Viewer.

Partners

This table displays all of the partners of this Corente Services Gateway, including Intranet, Extranet, and IPSec-based Client Partners. Addressing information for Clients is displayed only if they are currently connected to the Corente Services Gateway.

Note

If the addressing information does not display, the partner is not available for network connectivity testing. The **Connection**, **Ping**, and **Traceroute** buttons are not available.

Additionally, network connectivity testing is not available for any third party devices.

Name	The name of the partner.
IP Address	The visible IP address assigned to the partner.
Ping	Whether or not the **WAN** or **WAN/LAN** Ethernet interface of this Corente Services Gateway was able to successfully ping this partner when the **Test** page was loaded.
Test	Click the **Connection** button to run a simple connection test to this parter that will provide a descriptive, non-technical result. Click the **Ping** button to ping the IP address of this partner. Click the **Traceroute** button to traceroute to the IP address of this entity. Click the **Mtr** button to MTR to the IP address of this entity. The results of the test that you select will be displayed on a new page in Gateway Viewer.

17.6.3 Control

The **Machine and Server Control** page can be used to perform the following operations:

- **START Service**
- **RESTART Service**
- **STOP Service**
- **REBOOT Machine**
- **SHUTDOWN Machine**
- **FAILOVER Machine**
- **FAILOVER to Secondary WAN Interface**
- **FAILBACK to Primary WAN Interface**

To perform an operation, set the button for the desired operation and then click the **Submit** button directly below the selection. Any selection made from this page will present a confirmation screen that describes the selected operation and its consequences. Clicking **Cancel** will cancel the operation, while **Continue** will complete the operation and display its results.

The **FAILOVER Machine** option will be enabled only if **Hardware Failover** (also known as **Redundant Hardware**) has been configured for this Corente Services Gateway. Selecting this option will cause the Corente Services Gateway hardware to alternate between which gateway is currently Active and which is Standby.

The **FAILOVER to Secondary WAN Interface** and **FAILBACK to Primary WAN Interface** options will be available only if the Dual WAN feature has been configured for this Corente Services Gateway. Only one option will be selectable at a time, depending on which WAN interface (primary or secondary) is currently active. When you select **FAILOVER to Secondary WAN Interface** and click **Submit**, the Corente Services Gateway will restart and attempt to use the secondary WAN interface as its WAN connection. The secondary WAN interface will remain the active WAN interface until the secondary WAN interface fails, the gateway is restarted, or you return to this page and use the **FAILBACK to Primary WAN Interface** option. Use of the secondary WAN interface is not static upon restart of the Corente Services Gateway service or hardware. When the service or hardware is started, restarted, or rebooted, the Corente Services Gateway will attempt to detect both WAN interfaces, and will always attempt to use the primary WAN interface first. If both the primary and secondary WAN connections are unusable, the Corente Services Gateway will continuously reboot until one of the WAN connections is functional. The WAN interface that is currently in use will be displayed at the top of the **Active Corente Gateway WAN Interface** table.

Keep in mind that executing any of the operations on this page (except **START Service**) will cause an interruption of Corente Services Gateway service for this location. This location will be disconnected from the services and any in-progress communications over the secure application network will be interrupted. Consequently such interruptions should be planned for off hours.

The current status of the Corente Services Gateway service for this location will be indicated in parentheses at the top of the **Corente Gateway Service** table.

Note

Performing these operations on an **Inline** Corente Services Gateway has additional implications because of the additional services that an Inline Corente Services Gateway can provide. For example, the **Firewall State** and **Internet Connection**

> **Sharing (ICS) State**of the Corente Services Gateway will be maintained when you **STOP Service**. However, **SHUTDOWN** or **REBOOT** of an Inline Corente Services Gateway will interrupt these services, including the LAN gateway function that this machine performs. This means that all communications between machines on the local network will be disabled, as well as communication with machines in any location on the secure network or public network (Internet).

17.6.4 Remote Login

The **Remote Login Administration** page allows you to enable or disable remote login access from the Corente Services Control Point (SCP) to your Corente Services Gateway over the secure Corente SCP connection. Technical support personnel may request this access if you are having problems with your secure application network.

- If you want to prevent remote login access to this Corente Services Gateway from the Corente SCP, check the **Disable remote login access** box and then click the **Submit** button. This is the default setting.
- If you want to enable remote login access from the Corente SCP for an indefinite period of time, check the **Enable remote login access with no timeout** box and then click the **Submit** button.
- If you want to enable remote login access from the Corente SCP for a specified period of time and then have it automatically return to the disabled state, check the **Enable remote login access for ___ minutes** box. Enter the period of time (in minutes) that this access will remain enabled. Then click the **Submit** button.

Your current setting will be highlighted in gray.

17.6.5 Download

The **Corente Gateway download** page can be used to download all of the log files for a Corente Services Gateway and the text files for any of the SNMP MIBs that are supported by the Corente Services Gateway.

- Customer Care may request that you obtain all of the log files from a Corente Services Gateway and send them to Customer Care for analysis. This page automates that process. When you click the **Download** button in the **Corente Gateway Download Log Files** section, the Gateway Viewer will gather all relevant log files, create a compressed archive file, and download that archive file to the hard disk of the PC that you are using to access the Gateway Viewer application. You can then email the compressed file to Customer Care.
- The **Corente Gateway MIB files** section lists all of the SNMP MIBs that are available on the Corente Services Gateway. When you select a MIB and click the **Download** button, you can download the text file for that MIB onto the PC that you are currently using and view its object definitions. If you are using a special program on your PC to monitor the Corente Services Gateway with SNMP, you can install the text files for your chosen MIBs in that program. If you are querying the Corente Services Gateway manually, you can use the text files as guides to what objects and information are available through the MIB.

  To view only the MIBs that can provide specifial information about this Corente Services Gateway, select the option labeled **Show only Corente specific MIBs**. When this option is not selected, all supported MIBs will be shown.

17.6.6 Version

The **Corente Gateway Software Version Information** page displays a list of all the software that is installed on this Corente Services Gateway and each software package's version number.

Each software package is listed on this page as a hyperlink. When you click the hyperlink for a software package, a new page will be displayed that provides information about this package as well as a change log that details the history of the package on this Corente Services Gateway. Everytime a change is made to the software package, the change will be recorded in this log. This will allow you to view when a software package has been upgraded or modified.

17.7 Advanced

The options available in the **Advanced** menu lets you view the Corente Services Gateway configuration file, log file, history file, and thread information. You can also change your password from the **Advanced** menu. The options in this menu are intended for use by administrators only.

When you attempt to access an option from the **Advanced** menu, a dialog box may appear that requests a user name and password. Enter these items and click **OK**. You will only be asked for this information once per administration session. Your user name and password will be saved until you close your browser window.

The following options are be available from this menu:

- Section 17.7.1, “Display Configuration File of the Corente Services Gateway (or "Config")”
- Section 17.7.2, “Display Log File (Last 200 Lines) from the Corente Services Gateway Log File (or "Log")”
- Section 17.7.3, “Display History File (Last 200 Lines) from the Corente Services Gateway (or "History")”
- Section 17.7.4, “Display Thread Information for the Corente Services Gateway (or "Threads")”
- Section 17.7.5, “Change Password for the Administrator of the Corente Services Gateway (or "Change Password")”

17.7.1 Display Configuration File of the Corente Services Gateway (or "Config")

When you create a Corente Services Gateway, the configuration data is stored in a special file (downloaded to your floppy diskette) named `org.xml`. This item will display the contents of that file in your browser, except for information about the key which is removed for security purposes.

17.7.2 Display Log File (Last 200 Lines) from the Corente Services Gateway Log File (or "Log")

Displays the last 200 lines of the detailed debugging file `ORLOG.TXT`, with the digital signatures and modulus keys removed for readability. Customer Care may request to review this data when troubleshooting gateway problems.

17.7.3 Display History File (Last 200 Lines) from the Corente Services Gateway (or "History")

Displays the last 200 lines of the detailed history file ORHISTORY.TXT. The history file tracks gateway system events such as starts, stops, and upgrades. Customer Care may request to review this data when troubleshooting gateway problems.

17.7.4 Display Thread Information for the Corente Services Gateway (or "Threads")

The Corente Services Gateway is a multi-threaded application. Each thread performs a particular task. It is useful for debugging purposes to be able to determine the current state of these threads. This page will display the status and state of each individual thread within the application.

17.7.5 Change Password for the Administrator of the Corente Services Gateway (or "Change Password")

Certain operations of the Gateway Viewer are password protected. This item allows you to change the password associated with those pages. For security purposes you will need to know the current password in order to change it. You will not be able to change the user name.

Index

N

O

P

Q

R

S

T

U

W