Secure Router 4134/2330

Software Release 10.2.1 Release Notes

1. Release Summary

Release Date: April 6, 2010
Purpose: Software maintenance release to address customer found software issues.

2. Notes for Upgrade

Please see the technical documentation for the Secure Router 4134 and 2330 version 10.2 available at: http://www.nortel.com/support for details on how to upgrade your Secure Router unit.

When upgrading from 10.2 to this release if the user account's password was set in 10.2 and contains more than 9 characters, only the first 9 characters will be used after the upgrade.

File Names for This Release

Description	File Size	Version	File Name
Secure Router 4134 Application Image	29,070,684	10.2.1	SR4134.Z
Secure Router 2330 Application Image	30,055,731	10.2.1	SR2330.Z

3. Version of Previous Release

Software Version 10.2

4. Compatibility

N/A

5. New Features in the 10.2.1 Release

5.1 TCP MSS Clamping

The TCP MSS feature enables the configuration of the maximum segment size (MSS) for transient packets that traverse the interface. The **ip tcp-mss** command under the interface section specifies the MSS value on the intermediate router of the TCP SYN packets to avoid truncation. When a TCP SYN packet traverses the router the MSS option field in the packet is lowered to the value specified in the tcp-mss-clamping config.

The ability to set the TCP MSS value is supported on Ethernets, Bundles, AVC, L3-VLAN, Tunnels and firewall policy. Firewall policy level MSS clamping gives greater granularity by allowing the clamping to be performed only for certain hosts. When setting the TCP MSS value it is recommended that the MSS value is at least 40 bytes less than the MTU of the interface. The TCP header takes up 20 bytes of data (or more if options are used); the IP header also uses 20 or more bytes. This means that between them a minimum of 40 bytes are needed for headers, all of which is non-data "overhead".

WARNING

TCP MSS Clamping will not work on an Ethernet switch port, if the TCP connection originates from a switched Ethernet port on the router and its TCP destination is over another Ethernet switch port.

5.1.1 Configuring TCP MSS on a GRE/IPIP Tunnel Interface

Procedure Steps

Step	Action
1	To enter the configuration mode, enter: **`configure terminal`**
2	To select the tunnel, enter: **`interface tunnel <tunnel-name>`**
3	Specify the IP address for the tunnel, enter: **`[ip address <ipv4-address> <subnet-mask>] | [ipv6<ipv6-address>]`**
4	Specify the source address of the tunnel, enter: **`tunnel source <A.B.C.D>`**
5	Specify the destionation address of the tunnel, enter: **`tunnel destination <A.B.C.D>`**
6	Specify the tcp-mtu of the tunnel, enter: **`ip tcp-mss <value>`**
7	To exit the tunnel configuration mode, enter: **`exit`**

5.1.2 Configuring TCP MSS on an Ethernet Interface

Procedure Steps

Step	Action
1	To enter the configuration mode, enter: **`configure terminal`**
2	To select the ethernet, enter: **`interface ethernet  <slot/port number>`**
3	Specify the tcp-mtu of the ethernet, enter: **`ip tcp-mss <value>`**
4	To exit the ethernet configuration mode, enter: **`exit`**

5.2 QOS Strict Priority Queuing (SPQ)

Secure Router implements Strict Priority Queuing (SPQ) to minimize latency and jitter for traffic over Ethernet and Bundle interfaces. SPQ uses the shaping/scheduling infrastructure currently used with Class Based Queuing (CBQ), so there is minimal change to QoS configuration. Traffic is classified and marked as before using Policy-maps. Each traffic flow (class-map) is mapped to a priority queue. Multiple flows can be mapped to the same priority queue. When SPQ is enabled, instead of queuing the classified traffic into class queues, the traffic will flow through one of the interface queues based on the configuration. SPQ supports up to 8 queues per interface with pre-defined priorities. Queue 1 is highest priority queue while queue 8 is the lowest priority queue. All unclassified traffic is placed in queue 8 by default. SPQ can be enabled or disabled at the interface level for outbound flows. Only CBQ or SPQ can be active on any interface yet both can be active at the same time on different interfaces. SPQ is only supported on Ethernet, PPP, FR, MLPPP & MFR interfaces.

Unlike CBQ, where the committed rate percentage and peak rate percentage are specified globally in the class map, with SPQ, committed rate percentage is specified for each queue at the interface level with the shape command. The committed rate percentage can be configured between 0% (default) and 100% of the interface bandwidth. The peak rate percentage is 100% for all priority queues and cannot be modified. If the queues are configured with committed rates, they are serviced in round-robin mode. Any bandwidth available after all the committed rates are fulfilled is used to service the queues in strict-priority mode. Also, WRED can be configured on each queue for congestion control on Bundle interfaces. The latency for traffic for a SPQ queue can increase once it exceeds the committed rate percentage for that queue.

5.2.1 QOS SPQ CLI Commands

To configure SPQ, you must first setup up the policy map under the qos chassis section. A policy map consist of class maps where each class map is assigned a SPQ queue number with the assign-queue command. Shaping is configured for the queues using the shape command under interace queue section. When SPQ is enabled on an interface, the committed rate and peak rate percentages defined in the class map are ignored. All the clear and show commands are equivalent on SPQ as for CBQ.

5.2.2 Mapping a priority queue to a class map

Procedure Steps

Step	Action
1	To enter the configuration mode, enter: **configure terminal**
2	To select qos chassis, enter: **qos chassis**
3	Specify the policy map, enter: **policy-map <policy-map-name>**
4	Specify the class map, enter: **class-map <class-map-name>**
5	Specify which spq queue, enter: **assign-queue <queue number, range 1 - 8>**
6	To exit the class map configuration mode, enter: **exit**
7	To exit the policy map configuration mode, enter: **exit**

5.2.3 Configuring committed rate for priority queue on Ethernet interface

Procedure Steps

Step	Action
1	To enter the configuration mode, enter: **configure terminal**
2	To select the ethernet, enter: **interface ethernet <slot/port number>**
3	Specify qos chassis section, enter: **qos chassis**
4	Specify the SPQ Queue number, enter: **queue <queue number,range 1-8>**
5	Specify committed rate percentage, enter: **shape <committed rate percenaage,range 0 -100>**
6	To exit the queue configuration mode, enter: **exit**

5.2.4 Configuring RED for priority queue on Bundle interface

Procedure Steps

Step	Action
1	To enter the configuration mode, enter: **configure terminal**
2	To select the ethernet, enter: **interface bundle <bundle-name>**
3	Specify link info, enter: **link <interface-type> <interface number>**
4	Specify bundle encapsulation, enter: **encap <encap-type>**

5 Specify qos chassis section, enter:
```
qos chassis
```
6 Specify the SPQ Queue number, enter:
```
queue <queue number,range 1-8>
```
7 Specify RED thresholds for each drop precedence, enter:
```
red <drop-precedence> <min-threshold> <max-threshold> <drop
probability factor>
```
8 To enable RED on the queue, enter:
```
enable-red
```
9 To exit the queue configuration mode, enter:
```
exit
```

5.2.5 Enable SPQ on Ethernet Interface

Procedure Steps

Step	Action

1 To enter the configuration mode, enter:
```
configure terminal
```
2 To select the ethernet, enter:
```
interface ethernet  <slot/port number>
```
3 Specify qos chassis section, enter:
```
qos chassis
```
4 Enable SPQ, enter:
```
enable spq output
```

5.3 Mixed mode E1 Support for 8 port T1/E1 cards

The mixed mode E1 support allows for both E1 (31 channels per E1 port) and unframed E1 on the same 8 E1 port card. The 8 port card mixed E1 configurations are set through the carrier-type command like changing the card between E1 and T1. There are four new carrier types to support the mixed E1 configurations. In mixed mode, the channeled E1 ports are always first with the remaining ports set to unframed E1. There is **no** mixed mode for the small cards. The supported carrier types for 8 port T1/E1 cards mode settings are in the following table.

Carrier Type	Description
t1	8 T1 ports up to 16 channels per port
e1	8 E1 ports up to 16 channels per port
ue1	8 unframed E1 ports
c4u4	4 E1 ports up to 31 channels per port and 4 unframed E1 ports
c3u5	3 E1 ports up to 31 channels per port and 5 unframed E1 ports
c2u6	2 E1 ports up to 31 channels per port and 6 unframed E1 ports
c1u7	1 E1 ports up to 31 channels per port and 7 unframed E1 ports

PRI support has not changed and is only supported on the small cards.

To verify the carrier type currently active on a card the command ***show system configuration*** now shows the carrier type per card.

5.3.1 Setting the carrier type to 4 channelized E1 and 4 unframed ports on an 8 port T1/E1 card

Configure the carrier type for mixed E1 mode with 4 channelized E1 and 4 unframed ports. You must reboot the router in order for the configuration to take effect. For this mode, the parameter on the ***carrier-type*** command is ***c4u4***.

Procedure Steps

Step	Action
1	To enter the configuration mode, enter: **`configure terminal`**
2	To select the module and carrier type, enter: **`system carrier-type <slot> c4u4`**
3	To exit the configuration mode, enter: **`exit`**
4	To reboot the SR4134, enter: **`reboot`**

--End—

5.3.2 Setting the carrier type to 3 channelized E1 and 5 unframed ports on an 8 port T1/E1 card

Configure the carrier type for mixed E1 mode with 3 channelized E1 and 5unframed ports. You must reboot the router in order for the configuration to take effect. For this mode, the parameter on the ***carrier-type*** command is ***c3u5***.

Procedure Steps

Step	Action
1	To enter the configuration mode, enter: **`configure terminal`**
2	To select the module and carrier type, enter: **`system carrier-type <slot> c3u5`**
3	To exit the configuration mode, enter: **`exit`**
4	To reboot the SR4134, enter: **`reboot`**

--End—

5.3.3 Setting the carrier type to 2 channelized E1 and 6 unframed ports on an 8 port T1/E1 card

Configure the carrier type for mixed E1 mode with 2 channelized E1 and 6 unframed ports. You must reboot the router in order for the configuration to take effect. For this mode, the parameter on the ***carrier-type*** command is ***c2u6*****.**

Procedure Steps

Step	Action
1	To enter the configuration mode, enter: **configure terminal**
2	To select the module and carrier type, enter: **system carrier-type <slot> c2u6**
3	To exit the configuration mode, enter: **exit**
4	To reboot the SR4134, enter: **reboot**

--End—

5.3.4 Setting the carrier type to 1 channelized E1 and 7 unframed ports on an 8 port T1/E1 card

Configure the carrier type for mixed E1 mode with 1 channelized E1 and 7 unframed ports. You must reboot the router in order for the configuration to take effect. For this mode, the parameter on the ***carrier-type*** command is ***c1u7****.*

Procedure Steps

Step	Action
1	To enter the configuration mode, enter: **configure terminal**
2	To select the module and carrier type, enter: **system carrier-type <slot> c1u7**
3	To exit the configuration mode, enter: **exit**
4	To reboot the SR4134, enter: **reboot**

--End—

5.3.5 Hardware Changes for Mixed Mode E1 Support

The mixed mode E1 feature requires that 8 port T1/E1 cards have a new revision of CPLD so that all the ports work properly. The new CPLD revision is CPLD-Eng-Rev b. The ***show version*** command shows the revision number of the card as the last field on the row for the card. Below shows the output of the command:

SR# **show version**
show version
Runtime: 10.2.1.0
Created: Mar 24 2010, 20:24:18
Boot: 0.0.0.49 (NORMAL Boot)
NorBoot: 0.0.0.49
GolBoot: 0.0.0.49

Slot/SubSlot	Card-Type	Status	FPGA-Rev	FPGA-Eng-Rev	CPLD-Rev	CPLD-Eng-Rev	
0/-	MPU_A	NORMAL	0x1	0x3	---	0xb	
7/-	WTE_8	NORMAL	---	---	0x1	**0x9**	**← previous**
5/-	WTE_8	NORMAL	---	---	0x1	**0xb**	**← required**
4/-	WTE_2M	NORMAL	---	---	0x1	**0x6**	
1/-	WTE_2M	NORMAL	---	---	0x1	**0x5**	
2/-	WTE_1	NORMAL	---	---	0x1	**0x6**	

Resolution:

In order to enable Mixed mode E1 feature, upgrade to release 10.2.1 AND upgrade T1/E1 modules to the following revision:

SR0000011E5 - 8-port T1/E1 medium module: Upgrade to CPLD-Eng-Rev b

The process of upgrading T1/E1 cards can be initiated by calling 1-800-4NORTEL where a case and RMA will be created.

5.4 Avaya Aura Interoperability

Secure Router 2330 and 4134 survivable SIP-PSTN gateway feature is now interoperable with Avaya Aura 5.2.1 and 9600 series SIP phones. Please refer to support.avaya.com for a detailed application note on the usage.

5.5 Microsoft OCS R2 Interoperability

Secure Router 2330 and 4134 are compliant to Microsoft OCS R2 "Direct SIP : Basic Gateway" specifications.

5.6 DSP Enhancements

5.6.1 CLI command to control DTMF level

Syntax voice dsp dtmf-level
Parameter level - DTMF level adjustment in 0.1dB steps (enter as step-in-dB*10).
Range Between -60 and 70.
Default -3.3dBm
Description Configure outgoing DTMF level adjustments

5.6.2 CLI command to control DTMF twist

Syntax voice dsp dtmf-twist
Parameter twist - Amplitude twist value in 0.1dB steps (enter as step-in-dB*10).
Twist = AmpOfSecFreq - AmpOfPriFreq
Range Between -30 and 30.
Default -3.3dBm
Description Configure outgoing DTMF amplitude twist

5.6.3 CLI command to control the timeout duration

When the call is on hold & no RTCP is received for a configured duration, the call is disconnected. This CLI command can set the duration before the call is disconnected.

Syntax voice dsp no-rtcp-timeout
Parameter rtcp_timer - Value of timeout in seconds.
Range Between 1s and 2700s (45min)
Default 180s
Description Configure the timeout value

5.7 E1 R2 Enhancements

5.7.1 Backward Digit Configuration

To indicate variable number of digits a new character ‘R’ has been introduced in configuration of backward-digit. With this user can conveniently configure backward digit. ‘R’ indicates variable number of digits.

5.7.2 Incoming Call – variable DNIS

Secure Router can now accept variable number digits in Dialed Number Identification Service (DNIS) number or “dialed” number. For this backward-digits need to be configured as 1R31. Earlier behavior was to accept only fixed number of digits in DNIS. For example if backward digit is 11131 then SR was able to accept call with only 4 digits in DNIS.

‘R’ indicates variable number of digits.

For example, if peer makes use of dial plan shown below:

International Call – 12 digits
National Call – 10 digits
Local – 7 digits
Extension – 4 digits

For above calls then on SR backward digit needs to configured as 1R31.

In case if peer is configured to send ‘F’ indicating end of DNIS, then after receiving ‘F’ SR sends 3 (Group A backward signal) indicating number complete.

In case if peer is configured not to send ‘F’ to indicate no more DNIS digits to send then SR sends 3 (Group A backward signal) indicating number complete after interdigit timeout (default 6 seconds)

5.7.3 Incoming Call – request ANI

Secure Router can now be configured to request for Automatic Number Identification (ANI) or caller identification. Backward-digit needs to be configured as 1R61R31. The second ‘R’ in backward-digit configuration stands for variable number of digits in ANI.

Examples:

a. If peer is configured to send 4, 7, or 10 digits in ANI then backward-digit can be configured as '1R61R31' on SR.
b. If peer is configured to send fixed 4 digits in ANI then backward-digit can be configured as '1R61111131'. In this case after receiving 4 digits, SR will send '3' indication ANI is complete. If there are more digits in ANI then SR will ignore rest of the digits.

Below table shows backward digit configuration for various combinations of DNIS and ANI numbers/digits.

Call Direction	DNIS	ANI	Backward digit configuration
Incoming	4 (Fixed)	None	11131
Incoming	4 (Fixed)	4 (Fixed)	1113111131
Incoming	Variable	4 (Fixed)	1R6111131
Incoming	Variable	Variable	1R61R31
Incoming	4 (Fixed)	Variable	11161R31
Incoming	5 (Fixed)	None	111131
Incoming	5 (Fixed)	5 (Fixed)	111131111131
Incoming	Variable	5 (Fixed)	1R61111131
Incoming	Variable	Variable	1R61R31
Incoming	5 (Fixed)	Variable	111161R31

5.7.4 Inter-Digit Timeout Configuration

The default value of inter-digit timeout value is set to 6 seconds which is more realistic. Earlier it was 15 seconds that was too long and caller could hang up in the meantime. The parameter is now configurable for E1 R2 ports and can be configured using CLI 'timeout interdigit' under voice-port

5.8 Restrict the SIP Registrations to accept only provisioned users by SIP Survivability Module (SSM)

The "allow-backup-reg" command located under "voice service voip ssm registrar" CLI tree is enhanced to include a new parameter to restrict the SIP Registrations accepted by SIP Survivability Module (SSM) in backup mode. When this command is configured, SSM will only accept SIP Registrations from users configured using "subscriber" command located under "voice service voip ssm provisioning" CLI tree. The "show ssm registrar status" command will display the configuration of this allow-backup-reg command.

5.8.1 Restricting the SIP Registrations by SSM

Procedure Steps

Step Action

----

1 To enter the configuration mode, enter:
`configure terminal`

2 To select voip, enter:
`voice service voice`

3 Specify ssm, enter:
`ssm`

4 Specify restrict registration to provisioned users, enter:
`registrar allow-backup-reg provisioned-users`

5 To exit the ssm mode, enter:
`exit`

6 To exit the voip mode, enter:
```
exit
```
7 To exit the configuration mode, enter:
```
exit
```

5.9 FAT 32 File System Support for SR 4134 and 2330

Both the compact flash and USB drives can now support the FAT 32 file system. The file format command has an option parameter fat which can format the compact flash or usb to FAT 16 or 32.

5.9.1 Formatting USB drive for FAT 32 File System

Procedure Steps

Step	Action

1 To enter file mode, enter:
```
file
```
2 Insert USB drive into the SR 4134 router

3 Format the usb drive, enter:
```
format /usb0 32
```
4 Display the follow message and enter:
```
WARNING :
Do not remove the Compact Flash during this process
Do not reboot this device during this process

COMPACT FLASH FORMAT: Are you sure ? (y/n) :y
```
5 To exit the file mode, enter:
```
exit
```

5.9.2 Formatting an external compact flash for FAT 32 File System

Procedure Steps

Step	Action

1 To enter file mode, enter:
```
file
```
2 Insert compact drive into the router

3 Format the compact flash, enter:
```
format /cf1 32
```
4 Display the follow message and enter:
```
WARNING :
Do not remove the Compact Flash during this process
Do not reboot this device during this process

COMPACT FLASH FORMAT: Are you sure ? (y/n) :y
Erasing Compact Flash Blocks. Please wait till completed

Compact flash formatting completed
```
5 To exit the file mode, enter:
```
exit
```

6. Problems Resolved in the 10.2.1 Release

Bug Reference	Subsystem	Description
Q01988317	QOS	SLA monitoring feature does not report actual measured values
Q02060357-01	QOS	Crash when changing the atm bundle's pvc type without first deleting previous pvc type
Q02064022	Firewall	Can not support more than 1000 concurrent NAT sessions
Q02067596	Platform	Packet filter for an Ethernet switch port for TCP flags can causes tcp connection not to close properly
Q02067599	Platform	If both ACL and QOS are applied to an Ethernet switch port then ARP packets are dropped
Q02067603	Platform	Packet filter for an Ethernet switch port permitting ICMP packets of type icmptype3 does not work
Q02069537	VOIP	FXS lines stucks for a while if call transfer from SMC fails
Q02070727	Firewall	Crash when the serving a large number of concurrent SIP connections
Q02070980	Platform	Boot process does not complete with Mediation Server Module and no internal Packetized Voice Internal Module
Q02071049	Platform	Unable to see bundle stats when the bundle is down
Q02071747	Platform	In certain conditions, a DS0 link would have high latency and never recover
Q02073930	IPSEC	IP sec tunnels stop functioning after some time
Q02074470	SNMP	SNMP Server not responding to SNMP requests for other SNMP communities after deleting a SNMP community in certain cases
Q02076009	VOIP	TLS registered user call is rejected with 403
Q02080867	DHCP Server	DHCP Server could not work on vlan id which were larger than 99
Q02081347	VOIP	Dual-tone multi-frequency (**DTMF**) signaling packets were being dropped over an IPSec tunnel
Q02081384	Telnet	In certain conditions, the telnet banner can cause the router to be unreachable thru telnet
Q02081740	VOIP	Ringing tone distortion in case of FXS
Q02084398-01	SNMP	SNMP Server does not respond to source address if accessed through a tunnel
Q02084637	BGP	BGP distance parameter did not have any effect for IPv4 BPG neighbors
Q02086860	GRE	OSPF and RIP do not work over GRE IPIP Tunnel if the other side of GRE Tunnel is in different network
Q02094272-01	GRE	GRE IPIP Tunnel have slow performance
Q02096764	SNMP	The MIB variable for the bundle interface speed is incorrect and displays zero.
Q02102633	Platform	When displaying the summary line for reading the system.cfg at boot up is wrong if the display mode is set to 1.
Q02103478	IKE	IKE policies which included local_addr 0.0.0.0 and local_id would store improperly and error when the system.cfg was loaded
Q02103905	SIP Survivablity	1-7694181 - call transfer fails
Q02103907	SIP Survivablity	1-7671528 - Hold is not working properly if the call was forked by sip server
Q02107816	PPP	PPP with CHAP requires "peer-username" to be configured
Q02109590-01	RIP	Infrequent Crash caused by doing shut and no shut on a bundle where RIP is enabled
Q02111460	Platform	Crash when users telnets to the Quote of the Day Port (port 17) when firewall is not configured
Q02114382	VOIP	The "No codec" command is not working properly for certain scenarios
Q02114726	VOIP	VOIP Gateway not sending the right cause and message to ISDN.

Q02115304-01	SSH Server	Infrequent Crash caused when SSH session is not logged in and timeouts out
Q02122094	VOIP	The 'show dial peer voice <tag>' command does not display configured auth parameters
Q02122098	VOIP	Default codec deleted from codec pref list using no-command are not saved
Q02122377	SNMP	SNMP Server are sending deprecated BGP traps

7. Outstanding Issues

Refer to the previous Release Notes.

8. Known Limitations

Refer to the previous Release Notes
When using the firewall SIP ALG the remote SIP Server needs to be configured to use the same source port number that the connection request came on.

9. Documentation Corrections

On page 113 of the **Nortel Secure Router 2330/4134 Performance Management — Quality of Service NN47263-601 03.01** Manual for Release 10.2, the shaping parameter maximum range was wrong. under the procedure **Configuring interface shaping parameters.** The CBQ QoS interface limit for has been increase from 50000 to 100000 kilobytes. SBQ interface limit also supports the same limit in this release.

10. Notes

When configuring ipsec policy under the contivity-iras tree, the proposal:lifetime:kilobytes option has been depricated. This is because the Contivity client does not support IPsec SA lifetimes in kilobytes. This change does not affect the `crypto ipsec policies` or the `crypto dyanamic ipsec policies`.
The number of Static ARP entries has been expanded from 100 to 500 entries.

Warranty

Avaya provides a limited warranty on this product. Refer to your sales agreement to establish the terms of the limited warranty. In addition, Avaya's standard warranty language, as well as information regarding support for this product, while under warranty, is available to Avaya customers and other parties through the Avaya Support Web site: http://www.avaya.com/support

Please note that if you acquired the product from an authorized reseller, the warranty is provided to you by said reseller and not by Avaya.

Licenses

THE SOFTWARE LICENSE TERMS AVAILABLE ON THE AVAYA WEBSITE, HTTP://SUPPORT.AVAYA.COM/LICENSEINFO/ ARE APPLICABLE TO ANYONE WHO DOWNLOADS, USES AND/OR INSTALLS AVAYA SOFTWARE, PURCHASED FROM AVAYA INC., ANY AVAYA AFFILIATE, OR AN AUTHORIZED AVAYA RESELLER (AS APPLICABLE) UNDER A COMMERCIAL AGREEMENT WITH AVAYA OR AN AUTHORIZED AVAYA RESELLER. UNLESS OTHERWISE AGREED TO BY AVAYA IN WRITING, AVAYA DOES NOT EXTEND THIS LICENSE IF THE SOFTWARE WAS OBTAINED FROM ANYONE OTHER THAN AVAYA, AN AVAYA AFFILIATE OR AN AVAYA AUTHORIZED RESELLER, AND AVAYA RESERVES THE RIGHT TO TAKE LEGAL ACTION AGAINST YOU AND ANYONE ELSE USING OR SELLING THE SOFTWARE WITHOUT A LICENSE. BY INSTALLING, DOWNLOADING OR USING THE SOFTWARE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE INSTALLING, DOWNLOADING OR USING THE SOFTWARE (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THESE TERMS AND CONDITIONS AND CREATE A BINDING CONTRACT BETWEEN YOU AND AVAYA INC. OR THE APPLICABLE AVAYA AFFILIATE ("AVAYA").

Copyright

Except where expressly stated otherwise, no use should be made of the Documentation(s) and Product(s) provided by Avaya. All content in this documentation(s) and the product(s) provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software. Unauthorized reproduction, transmission, dissemination, storage, and or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Third Party Components

Certain software programs or portions thereof included in the Product may contain software distributed under third party agreements ("Third Party Components"), which may contain terms that expand or limit rights to use certain portions of the Product ("Third Party Terms"). Information regarding distributed Linux OS source code (for those Products that have distributed the Linux OS source code), and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply to them is available on the Avaya Support Web site: http://support.avaya.com/Copyright