

# Serie VCS o Expressway Series Xconfig e Xstatus Output Collection con PuTTY

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Connetti da console](#)

[Connessione tramite SSH](#)

[VCS e serie Expressway x8.2](#)

[Verifica](#)

[Risoluzione dei problemi](#)

## Introduzione

In questo documento viene descritto come raccogliere l'output CLI dei comandi **xconfig** e **xstatus** da Video Communication Server (VCS) e dai dispositivi della serie Expressway, quali VCS-Control, VCS-Expressway, Expressway-C e Expressway-E, che Cisco Technical Assistance Center (TAC) deve recuperare occasionalmente.

## Prerequisiti

### Requisiti

Cisco raccomanda la conoscenza dei seguenti argomenti:

- PuTTY o software di emulazione terminale simile, come SecureCRT, Tera Term, o simile.
- Nome utente e password dell'account amministratore per il dispositivo serie VCS/Expressway.
- Cavo console seriale RJ45-D-Sub9pin o SSH (Secure Shell) consentito nel percorso di rete.

### Componenti usati

Le informazioni fornite in questo documento si basano sulle seguenti versioni software e hardware:

- PuTTY (per ottenerne una copia, visitare la [pagina di download di PuTTY](#)).
- Nell'esempio viene utilizzato un software VCS-C con versione 7.2.1 applicabile alla versione

8.2.2, la più recente al momento.

## Configurazione

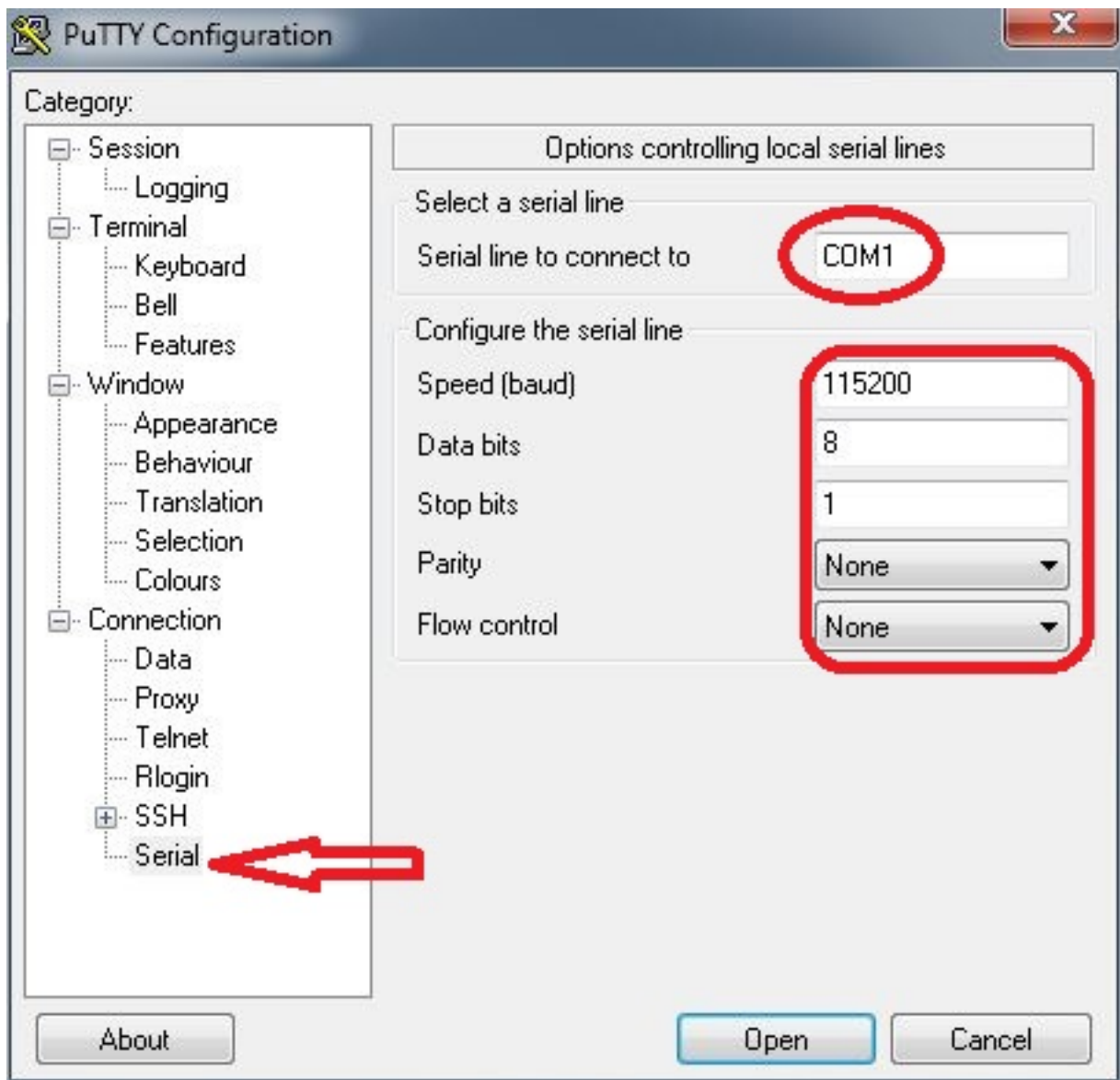
### Connetti da console

**Nota:** In questo articolo si presume che sia stato collegato un cavo console seriale fisico funzionale. Dovrebbe averne ricevuto uno con il dispositivo.

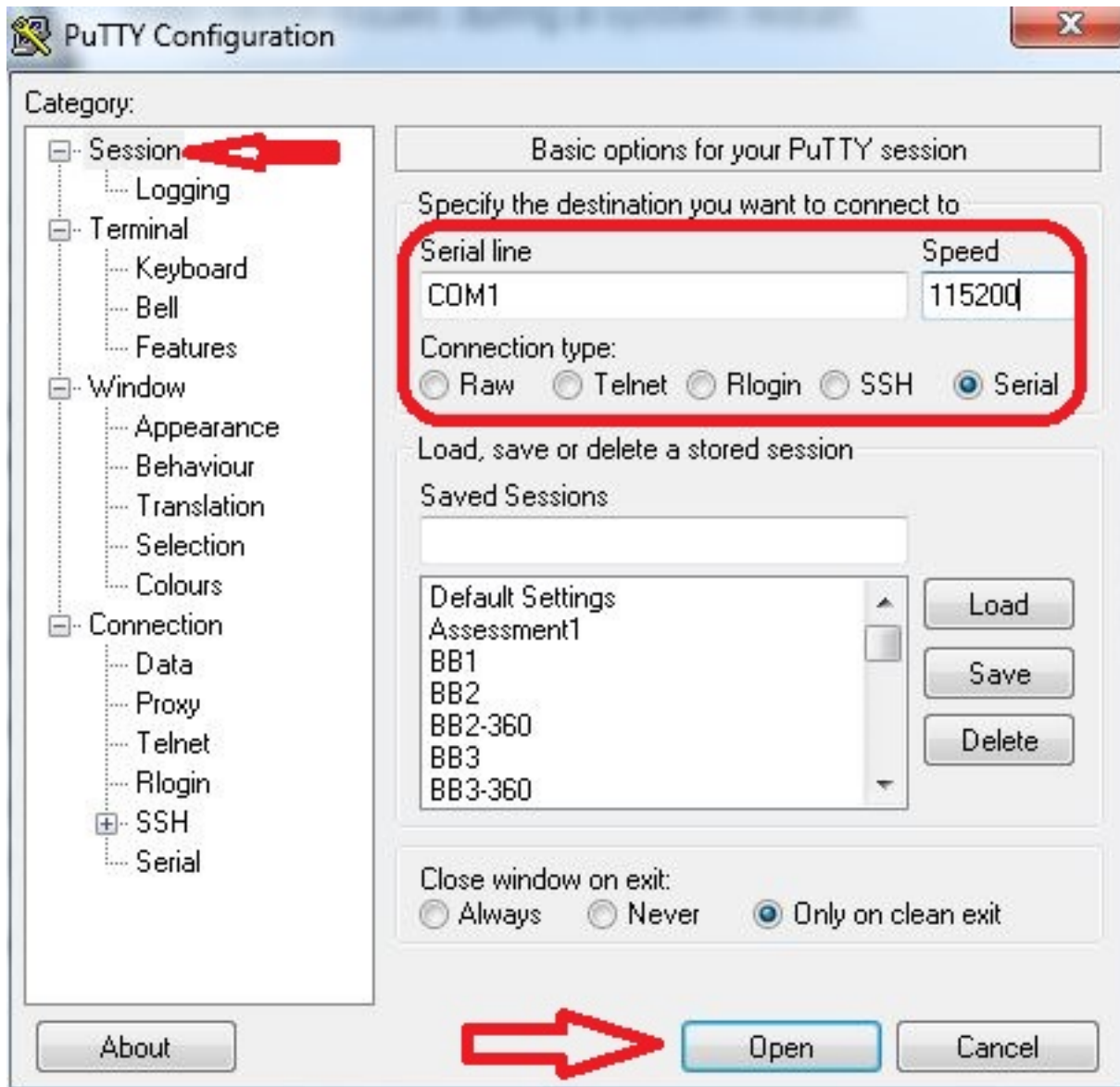
Di seguito è riportato un esempio delle impostazioni che è necessario configurare per l'accesso alla console seriale in PuTTY.

**Nota:** Sarà necessario regolare la porta COM (Communication) in base al modo in cui la console è collegata al PC.

1. Selezionare **Configuration > Category > Connection > Serial** e regolare le impostazioni seriali come mostrato di seguito:



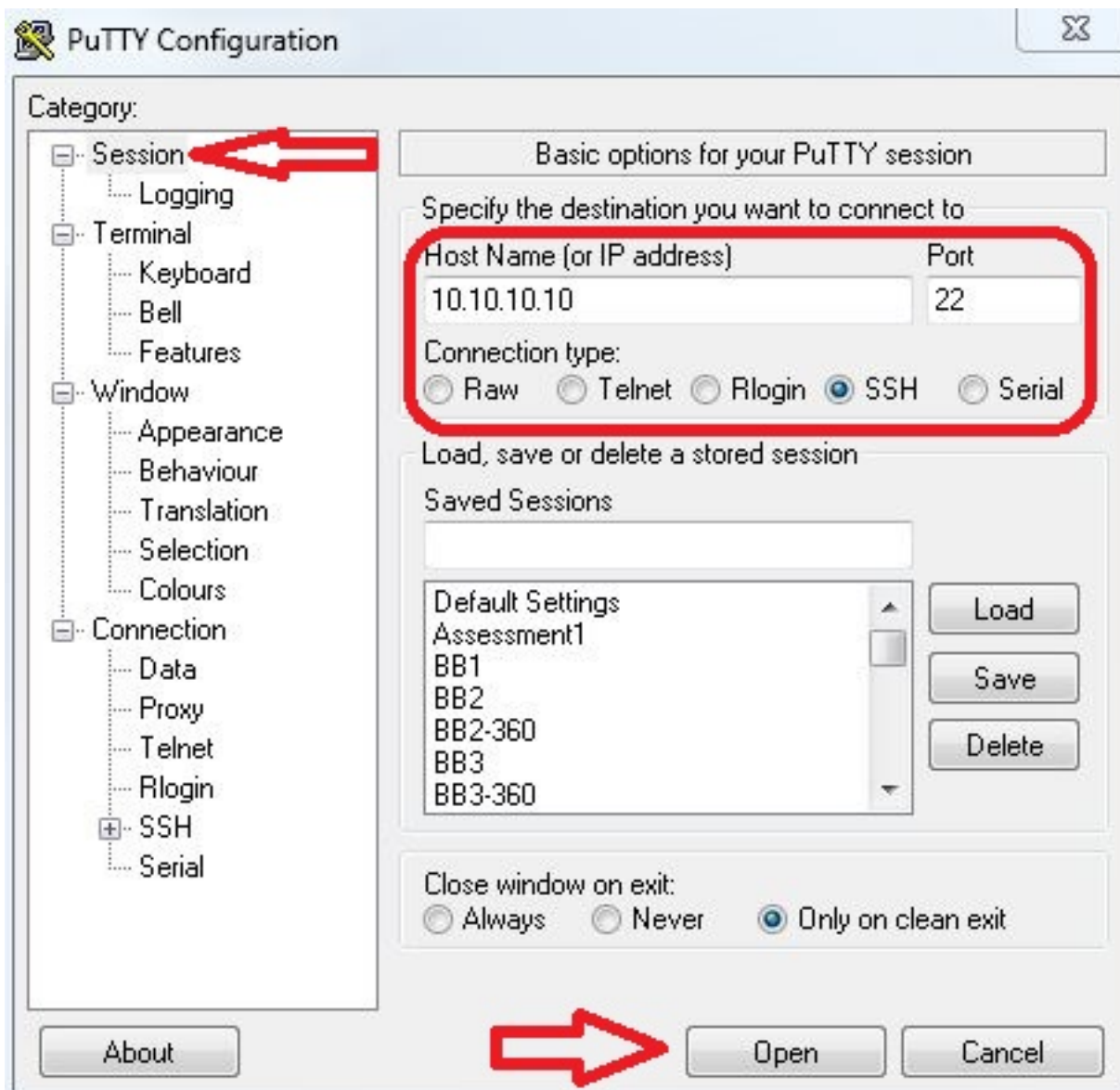
2. Selezionare **Categoria > Sessione**, selezionare **Serial type** (Tipo di serie) come tipo di connessione, quindi fare clic su **Open (Apri)** come mostrato di seguito:



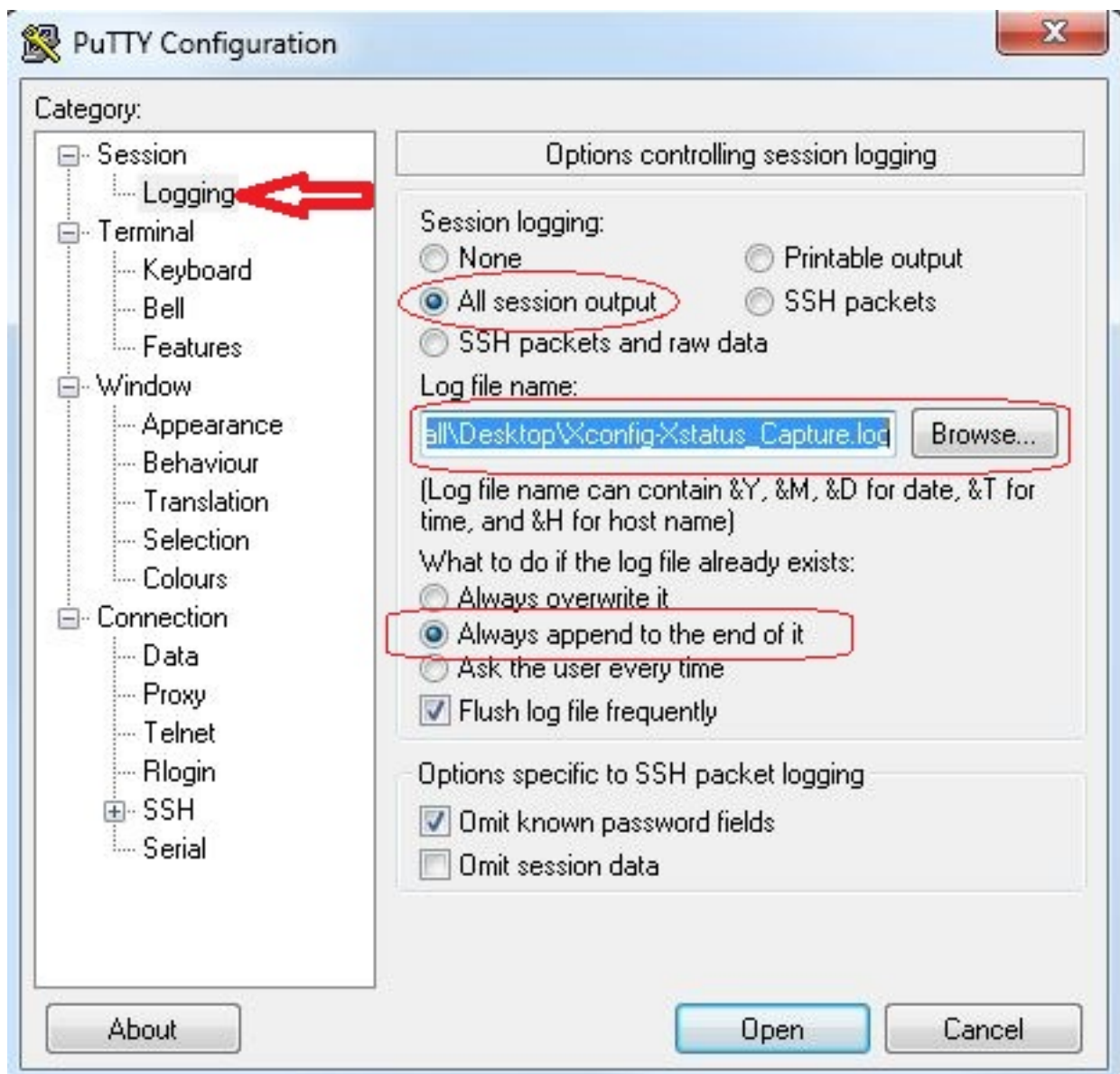
## Connessione tramite SSH

In alternativa, è possibile configurare il supporto SSH nel dispositivo.

1. Utilizzare l'indirizzo IP del dispositivo VCS/Expressway per regolare le impostazioni in PuTTY, come mostrato nell'esempio:



2. Prima o durante la sessione PuTTY sul dispositivo, è necessario impostare le impostazioni di registrazione. A tale scopo, selezionare **Configurazione > Categoria > Sessione > Registrazione** e configurare le impostazioni in modo che corrispondano a questo esempio (modificare il percorso e il nome del file in base al PC in uso e alle esigenze):



3. Dopo la connessione e l'accesso, viene visualizzata una schermata simile a questa. Accedere come amministratore come indicato qui.

```
VCSorExpressway - PuTTY
login as: admin
Using keyboard-interactive authentication.
Password:

5 alarms:
 * error      Insecure password in use - The admin user has the default password
 set
 * warning    Security alert - The TMS agent database has the default LDAP passw
 ord set
 * warning    Configuration warning - The VCS is running in a legacy TMS Agent m
 ode; you are recommended to switch your system to use a different mode
 * warning    Insecure password in use - The root user has the default password
 set
 * warning    Security alert - The TMS agent database has the default replicatio
 n password set

Last login: Thu Jun 19 08:12:21 EDT 2014
Welcome to VCS1-Control
TANDBERG VCS Release X7.2.1
SW Release Date: 2012-09-25

OK
```

**Attenzione:** Poiché si tratta di un ambiente lab, gli allarmi possono essere ignorati. Se l'allarme si verifica in un ambiente di produzione, deve essere risolto il prima possibile.

4. Digitare il comando **xstatus** e premere **Invio**:

```
VCSorExpressway - PuTTY
login as: admin
Using keyboard-interactive authentication.
Password:

5 alarms:
 * error      Insecure password in use - The admin user has the default password
 set
 * warning    Security alert - The TMS agent database has the default LDAP passw
 ord set
 * warning    Configuration warning - The VCS is running in a legacy TMS Agent m
 ode; you are recommended to switch your system to use a different mode
 * warning    Insecure password in use - The root user has the default password
 set
 * warning    Security alert - The TMS agent database has the default replicatio
 n password set

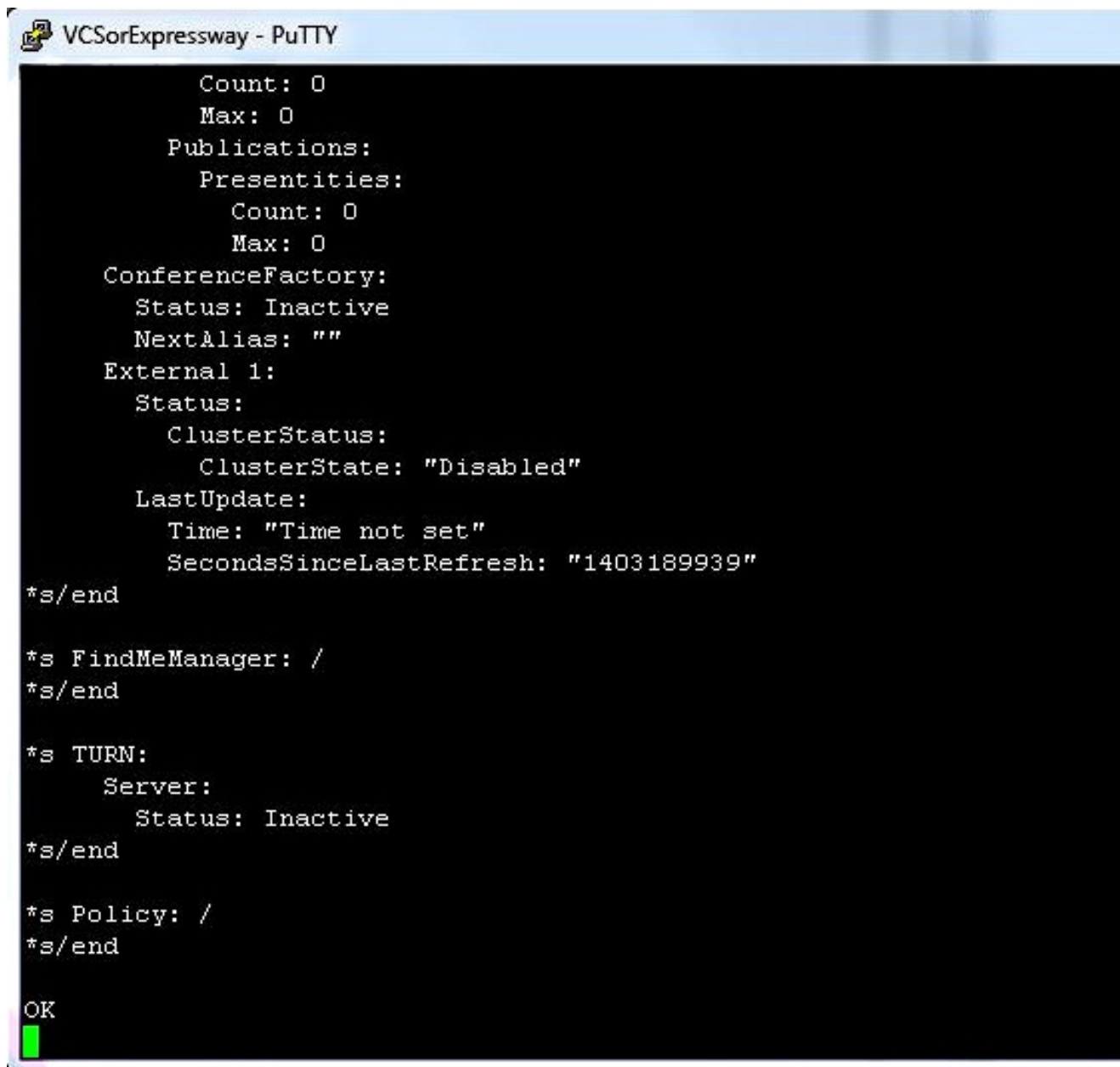
Last login: Thu Jun 19 08:12:21 EDT 2014
Welcome to VCS1-Control
TANDBERG VCS Release X7.2.1
SW Release Date: 2012-09-25

OK

xstatus
```

Di seguito è riportato l'output **xstatus** che viene visualizzato dopo aver premuto Invio. L'output scorre troppo rapidamente per essere visualizzato fino alla fine. Finché la

registrazione è stata configurata in precedenza, si troverà nel file di testo.



```
VCSorExpressway - PuTTY
    Count: 0
    Max: 0
  Publications:
    Presentities:
      Count: 0
      Max: 0
ConferenceFactory:
  Status: Inactive
  NextAlias: ""
External 1:
  Status:
    ClusterStatus:
      ClusterState: "Disabled"
  LastUpdate:
    Time: "Time not set"
    SecondsSinceLastRefresh: "1403189939"
*s/end

*s FindMeManager: /
*s/end

*s TURN:
  Server:
    Status: Inactive
*s/end

*s Policy: /
*s/end

OK
```

Dopo aver raccolto l'output del comando **xstatus**, è possibile raccogliere l'output del comando **xconfig**.

5. Digitare il comando **xconfig** e premere **Invio**.

```
xconfig
```

Di seguito è riportato un esempio dell'output **xconfig** dopo aver premuto invio. L'output è passato troppo rapidamente per essere visualizzato fino alla fine. Finché la registrazione è stata configurata in precedenza, il file di testo sarà vuoto.



```
fe xConfiguration Policy AdministratorPolicy Service Server 3 Address: ""
fe xConfiguration Policy AdministratorPolicy Service Path: ""
fe xConfiguration Policy AdministratorPolicy Service Status Path: "status"
fe xConfiguration Policy AdministratorPolicy Service UserName: ""
fe xConfiguration Policy AdministratorPolicy Service Password: "(cipher)
fe xConfiguration Policy AdministratorPolicy Service DefaultCPL: "<reject status='504' reason='Admin Policy Unavailabl
e' />"
fe xConfiguration Policy FindMe Mode: Off
fe xConfiguration Policy FindMe CallerId: IncomingID
fe xConfiguration Policy FindMe UserDeviceRestriction: Off
fe xConfiguration Applications ConferenceFactory Mode: Off
fe xConfiguration Applications ConferenceFactory Alias: ""
fe xConfiguration Applications ConferenceFactory Template: ""
fe xConfiguration Applications ConferenceFactory Range Start: 1
fe xConfiguration Applications ConferenceFactory Range End: 65535
fe xConfiguration Applications OCS Relay Mode: Off
fe xConfiguration Applications OCS Relay OCS Domain: ""
fe xConfiguration Applications OCS Relay OCS Routing Prefix: "ocs"
fe xConfiguration Applications Presence Server Mode: Off
fe xConfiguration Applications Presence Server Publication ExpireDelta: 1800
fe xConfiguration Applications Presence Server Subscription ExpireDelta: 3600
fe xConfiguration Applications Presence User Agent Mode: Off
fe xConfiguration Applications Presence User Agent ExpireDelta: 3600
fe xConfiguration Applications Presence User Agent RetryDelta: 1800
fe xConfiguration Applications Presence User Agent Presentity Idle Status: Online
fe xConfiguration ResourceUsage Warning Activation Level: 90
fe xConfiguration Services AdvancedMediaGateway Zone Name: ""
fe xConfiguration Services AdvancedMediaGateway Policy Mode: Off
OK
```

## VCS e serie Expressway x8.2

Nella versione software di x8.2, **xconfiguration** e **xstatus** sono ora inclusi quando viene eseguito un log di diagnostica.

1. Selezionare **Manutenzione > Diagnostica > Registrazione diagnostica**.
2. Selezionare **Avvia nuovo registro** e quindi **Interrompi registrazione** immediatamente.

**Nota:** Questo metodo contiene anche il file **logging snapshot.txt** che registra i messaggi in risposta alle attività che si svolgono su VCS o Expressway Series in quel momento.

L'archivio dei log di diagnostica scaricato contiene i seguenti file:

**logging snapshot.txt** - Contiene messaggi di log in risposta alle attività eseguite durante il periodo di logging.

**xconf\_dump.txt** - Contiene informazioni sulla configurazione del sistema al momento dell'avvio della registrazione.

**xstat\_dump.txt** - Contiene informazioni sullo stato del sistema al momento dell'avvio della registrazione.

(se pertinente) **diagnostic\_logging\_tcpdump.pcap** - Contiene i pacchetti acquisiti durante il periodo di registrazione.

## Verifica

Di seguito è riportato un esempio dell'aspetto dell'output **xstatus** e **xconfig** nel file di testo salvato con le impostazioni di registrazione:

xstatus

```
*s SystemUnit:
  Product: "TANDBERG VCS"
  Uptime: 24963390
  SystemTime: "2014-06-19 14:58:59"
  TimeZone: "US/Eastern"
  LocalTime: "2014-06-19 10:58:59"
  Software:
    Version: "X7.2.1"
    Build: "296181"
    Name: "s42700"
    ReleaseDate: "2012-09-25"
    ReleaseKey: "*****"
  Configuration:
    NonTraversalCalls: 500
    TraversalCalls: 200
    Registrations: 2500
    Expressway: False
    Encryption: True
    Interworking: True
    FindMe: True
    DeviceProvisioning: True
    DualNetworkInterfaces: False
    AdvancedAccountSecurity: False
    StarterPack: False
    EnhancedOCSCollaboration: True
  Hardware:
    Version: "VMWare"
    SerialNumber: "*****"
*s/end

*s Ethernet 1:
  MacAddress: "00:50:56:A1:70:06"
  Speed: 10000full
  IPv4:
    Address: "10.10.10.10"
    SubnetMask: "255.255.255.0"
*s/end

*s Ethernet 2:
  MacAddress: "00:50:56:A1:70:04"
  Speed: 10000full
  IPv4:
    Address: "192.168.0.100"
    SubnetMask: "255.255.255.0"
*s/end

*s Options:
  Option 1:
    Key: "116341X300-1-!!!!!!!"
    Description: "300 Non-traversal Calls"
  Option 2:
    Key: "116341P00-1-!!!!!!!"
    Description: "Device Provisioning"
  Option 3:
    Key: "116341G00-1-!!!!!!!"
    Description: "H323-SIP Interworking Gateway"
  Option 4:
```

```
Key: "116341U00-1-!!!!!!!"
Description: "FindMe"
Option 5:
Key: "116341C00-1-!!!!!!!"
Description: "Enhanced OCS Collaboration"
Option 8:
Key: "116341Y200-1-!!!!!!!"
Description: "200 Traversal Calls"
Option 9:
Key: "116341X200-1-!!!!!!!"
Description: "200 Non-traversal Calls"
*s/end

*s IP:
Protocol: IPv4
IPv4:
Gateway: "10.10.10.1"
*s/end

*s ExternalManager:
Status: Active
Address: "10.10.10.104"
Protocol: HTTP
URL: "tms/public/external/management/systemmanagementservice.asmx"
*s/end

*s Feedback 1:
Status: Off
*s/end

*s Feedback 2:
Status: Off
*s/end

*s Feedback 3:
Status: On
URL: "http://10.10.10.104/tms/public/feedback/code.aspx"
Expression: "/Event/CallDisconnected"
Expression: "/Event/CallConnected"
Expression: "/Event/CallFailure"
Expression: "/Event/RegistrationAdded"
Expression: "/Event/RegistrationChanged"
Expression: "/Event/ResourceUsage"
Expression: "/Event/AuthenticationFailure"
Expression: "/Status/Warnings"
*s/end

*s ResourceUsage:
Calls:
Traversal:
Current: 0
Max: 0
Total: 0
NonTraversal:
Current: 0
Max: 1
Total: 2
Registrations:
Current: 0
Max: 3
Total: 42
*s/end

*s Calls: /
```

\*s/end

\*s Zones:

DefaultZone:

Name: "DefaultZone"

Bandwidth:

LocalUsage: 0

ClusterUsage: 0

LocalZone:

DefaultSubZone:

Name: "DefaultSubZone"

Bandwidth:

LocalUsage: 0

ClusterUsage: 0

TraversalSubZone:

Name: "TraversalSubZone"

Bandwidth:

LocalUsage: 0

ClusterUsage: 0

ClusterSubZone:

Name: "ClusterSubZone"

Bandwidth:

LocalUsage: 0

ClusterUsage: 0

Searches:

Current: 0

CurrentDirected: 0

Total: 64081

Dropped: 0

MaxSubSearchExceeded: 0

MaxTargetsExceeded: 0

Zone 1:

Name: "TraversalZone"

Bandwidth:

LocalUsage: 0

ClusterUsage: 0

Status: Active

Type: TraversalClient

TraversalClient:

Peer 1:

H323:

Status: Active

Address: "10.10.10.102"

Port: 6001

LastStatusChange: "2014-04-03 09:50:35"

SIP:

Status: Active

Address: "10.10.10.102"

Port: 7001

LastStatusChange: "2014-04-03 09:49:13"

Server: "TANDBERG/4102 (X7.0)"

\*s/end

\*s Alternates: /

\*s/end

\*s Links:

Link 1:

Name: "DefaultSZtoTraversalSZ"

Bandwidth:

LocalUsage: 0

ClusterUsage: 0

Link 2:

Name: "DefaultSZtoDefaultZ"

```
Bandwidth:
  LocalUsage: 0
  ClusterUsage: 0
Link 3:
  Name: "DefaultSZtoClusterSZ"
  Bandwidth:
    LocalUsage: 0
    ClusterUsage: 0
Link 4:
  Name: "TraversalSZtoDefaultZ"
  Bandwidth:
    LocalUsage: 0
    ClusterUsage: 0
Link 5:
  Name: "Zone001ToTraversalSZ"
  Bandwidth:
    LocalUsage: 0
    ClusterUsage: 0
*s/end

*s Pipes: /
*s/end

*s Registrations: /
*s/end

*s SIP:
  Ethernet 1:
    IPv4:
      UDP:
        Status: Inactive
      TCP:
        Status: Active
        Address: "10.10.10.10:5060"
      TLS:
        Status: Active
        Address: "10.10.10.10:5061"
    IPv6:
      UDP:
        Status: Inactive
      TCP:
        Status: Inactive
      TLS:
        Status: Inactive
  Ethernet 2:
    IPv4:
      UDP:
        Status: Inactive
      TCP:
        Status: Inactive
      TLS:
        Status: Inactive
    IPv6:
      UDP:
        Status: Inactive
      TCP:
        Status: Inactive
      TLS:
        Status: Inactive
  Transport:
    Server 19857:
      Socket:
        Type: "SERV_UDP"
        State: "INUSE"
```

ID:  
  Local: 85393  
  Global: 0  
Buffer:  
  Input:  
    Length: 20000  
  Output:  
    Length: 20000  
Local:  
  Address: "127.0.0.1:5060"  
Remote:  
  Address: ""  
Network:  
  Number: 1  
Certificate:  
  Subject:  
    Name: ""  
TLS:  
  Cipher:  
    Name: ""  
Last:  
  Packet:  
    Received: 0  
Close:  
  In: 20  
Secure: False  
X509:  
  Certificate:  
    Verified: False  
Queue:  
  Max:  
    Size: 0  
  Add:  
    Failures: 0  
Flow:  
  Token: ""  
Server 19856:  
Socket:  
  Type: "SERV\_TCP"  
  State: "INUSE"  
  ID:  
    Local: 150928  
    Global: 1  
  Buffer:  
    Input:  
      Length: 0  
    Output:  
      Length: 0  
Local:  
  Address: "127.0.0.1:5060"  
Remote:  
  Address: ""  
Network:  
  Number: 1  
Certificate:  
  Subject:  
    Name: ""  
TLS:  
  Cipher:  
    Name: ""  
Last:  
  Packet:  
    Received: 0  
Close:

In: 20  
Secure: False  
X509:  
Certificate:  
Verified: False  
Queue:  
Max:  
Size: 0  
Add:  
Failures: 0  
Flow:  
Token: ""  
Server 19855:  
Socket:  
Type: "SERV\_TLS"  
State: "INUSE"  
ID:  
Local: 216463  
Global: 2  
Buffer:  
Input:  
Length: 0  
Output:  
Length: 0  
Local:  
Address: "127.0.0.1:5061"  
Remote:  
Address: ""  
Network:  
Number: 1  
Certificate:  
Subject:  
Name: ""  
TLS:  
Cipher:  
Name: ""  
Last:  
Packet:  
Received: 0  
Close:  
In: 20  
Secure: True  
X509:  
Certificate:  
Verified: False  
Queue:  
Max:  
Size: 0  
Add:  
Failures: 0  
Flow:  
Token: ""  
Server 19854:  
Socket:  
Type: "SERV\_UDP"  
State: "INUSE"  
ID:  
Local: 281998  
Global: 3  
Buffer:  
Input:  
Length: 20000  
Output:  
Length: 20000

Local:  
  Address: "[::1]:5060"  
Remote:  
  Address: ""  
Network:  
  Number: 1  
Certificate:  
  Subject:  
    Name: ""  
TLS:  
  Cipher:  
    Name: ""  
Last:  
  Packet:  
    Received: 0  
Close:  
  In: 20  
Secure: False  
X509:  
  Certificate:  
    Verified: False  
Queue:  
  Max:  
    Size: 0  
  Add:  
    Failures: 0  
Flow:  
  Token: ""  
Server 19853:  
  Socket:  
    Type: "SERV\_TCP"  
    State: "INUSE"  
    ID:  
      Local: 347533  
      Global: 4  
    Buffer:  
      Input:  
        Length: 0  
      Output:  
        Length: 0  
Local:  
  Address: "[::1]:5060"  
Remote:  
  Address: ""  
Network:  
  Number: 1  
Certificate:  
  Subject:  
    Name: ""  
TLS:  
  Cipher:  
    Name: ""  
Last:  
  Packet:  
    Received: 0  
Close:  
  In: 20  
Secure: False  
X509:  
  Certificate:  
    Verified: False  
Queue:  
  Max:  
    Size: 0



Add:  
Failures: 0  
Flow:  
Token: ""  
Server 19852:  
Socket:  
Type: "SERV\_TLS"  
State: "INUSE"  
ID:  
Local: 413068  
Global: 5  
Buffer:  
Input:  
Length: 0  
Output:  
Length: 0  
Local:  
Address: "[::1]:5061"  
Remote:  
Address: ""  
Network:  
Number: 1  
Certificate:  
Subject:  
Name: ""  
TLS:  
Cipher:  
Name: ""  
Last:  
Packet:  
Received: 0  
Close:  
In: 20  
Secure: True  
X509:  
Certificate:  
Verified: False  
Queue:  
Max:  
Size: 0  
Add:  
Failures: 0  
Flow:  
Token: ""  
Server 19851:  
Socket:  
Type: "SERV\_TCP"  
State: "INUSE"  
ID:  
Local: 478603  
Global: 6  
Buffer:  
Input:  
Length: 0  
Output:  
Length: 0  
Local:  
Address: "10.10.10.10:5060"  
Remote:  
Address: ""  
Network:  
Number: 2  
Certificate:  
Subject:

Name: ""  
TLS:  
  Cipher:  
    Name: ""  
Last:  
  Packet:  
    Received: 0  
Close:  
  In: 20  
Secure: False  
X509:  
  Certificate:  
    Verified: False  
Queue:  
  Max:  
    Size: 0  
  Add:  
    Failures: 0  
Flow:  
  Token: ""  
Server 19850:  
  Socket:  
    Type: "SERV\_TLS"  
    State: "INUSE"  
    ID:  
      Local: 544138  
      Global: 7  
    Buffer:  
      Input:  
        Length: 0  
      Output:  
        Length: 0  
  Local:  
    Address: "10.10.10.10:5061"  
  Remote:  
    Address: ""  
  Network:  
    Number: 2  
  Certificate:  
    Subject:  
      Name: ""  
  TLS:  
    Cipher:  
      Name: ""  
  Last:  
    Packet:  
      Received: 0  
  Close:  
    In: 20  
  Secure: True  
  X509:  
    Certificate:  
      Verified: False  
  Queue:  
    Max:  
      Size: 0  
    Add:  
      Failures: 0  
  Flow:  
    Token: ""  
Client 7747:  
  Socket:  
    Type: "TLS\_OUTG"  
    State: "INUSE"

ID:  
Local: 825433667  
Global: 654  
Buffer:  
Input:  
Length: 5120  
Output:  
Length: 20000  
Local:  
Address: "10.10.10.10:27573"  
Remote:  
Address: "10.10.10.102:7001"  
Network:  
Number: 2  
Certificate:  
Subject:  
Name: ""  
TLS:  
Cipher:  
Name: "DHE-RSA-AES256-SHA"  
Last:  
Packet:  
Received: -1798628722  
Close:  
In: 900  
Secure: True  
X509:  
Certificate:  
Verified: False  
Queue:  
Max:  
Size: 1  
Add:  
Failures: 0  
Flow:  
Token: ""

\*s/end

\*s H323:

Registration:  
Status: Active  
IPv4:  
Address: "10.10.10.10:1719"  
CallSignaling:  
Status: Active  
IPv4:  
Address: "10.10.10.10:1720"  
Assent:  
CallSignaling:  
Status: Inactive  
H46018:  
CallSignaling:  
Status: Inactive

\*s/end

\*s Applications:

Presence:  
UserAgent:  
Status: Inactive  
Presentity:  
Count: 0  
Server:  
Subscriptions:  
Count: 0

Max: 0  
Expired: 0  
Subscribers:  
  Count: 0  
  Max: 0  
Status: Inactive  
Presentities:  
  Count: 0  
  Max: 0  
Publications:  
  Presentities:  
    Count: 0  
    Max: 0  
ConferenceFactory:  
  Status: Inactive  
  NextAlias: ""  
External 1:  
  Status:  
    ClusterStatus:  
      ClusterState: "Disabled"  
  LastUpdate:  
    Time: "Time not set"  
    SecondsSinceLastRefresh: "1403189939"

\*s/end

\*s FindMeManager: /

\*s/end

\*s TURN:

  Server:

    Status: Inactive

\*s/end

\*s Policy: /

\*s/end

OK

```
xcommand xconfig
*c xConfiguration Login Remote Protocol: LDAP
*c xConfiguration Login Remote LDAP Server Address: ""
*c xConfiguration Login Remote LDAP Server FQDNResolution: AddressRecord
*c xConfiguration Login Remote LDAP Server Port: 389
*c xConfiguration Login Remote LDAP VCS BindUsername: ""
*c xConfiguration Login Remote LDAP VCS BindPassword: "{cipher}XXXXXXXXXX
XXXXXXXXXXXX"
*c xConfiguration Login Remote LDAP VCS BindDN: ""
*c xConfiguration Login Remote LDAP BaseDN Accounts: ""
*c xConfiguration Login Remote LDAP BaseDN Groups: ""
*c xConfiguration Login Remote LDAP Encryption: Off
*c xConfiguration Login Remote LDAP SASL: DIGEST-MD5
*c xConfiguration Login Remote LDAP CRLCheck: None
*c xConfiguration Login Remote LDAP DirectoryType: ActiveDirectory
*c xConfiguration SystemUnit Name: "VCS1-Control"
*c xConfiguration SystemUnit Maintenance Mode: Off
*c xConfiguration Option 1 Key: "116341X300-1-!!!!!!!"
*c xConfiguration Option 2 Key: "116341P00-1-!!!!!!!"
*c xConfiguration Option 3 Key: "116341G00-1-!!!!!!!"
*c xConfiguration Option 4 Key: "116341U00-1-!!!!!!!"
*c xConfiguration Option 5 Key: "116341C00-1-!!!!!!!"
*c xConfiguration Option 8 Key: "116341Y200-1-!!!!!!!"
*c xConfiguration Option 9 Key: "116341X200-1-!!!!!!!"
*c xConfiguration Ethernet 1 Speed: Auto
*c xConfiguration Ethernet 1 IP V4 Address: "10.10.10.10"
*c xConfiguration Ethernet 1 IP V4 SubnetMask: "255.255.255.0"
*c xConfiguration Ethernet 1 IP V6 Address: ""
*c xConfiguration Ethernet 2 Speed: Auto
*c xConfiguration Ethernet 2 IP V4 Address: "192.168.0.100"
*c xConfiguration Ethernet 2 IP V4 SubnetMask: "255.255.255.0"
*c xConfiguration Ethernet 2 IP V6 Address: ""
*c xConfiguration IPProtocol: IPv4
*c xConfiguration IP Gateway: "10.10.10.1"
*c xConfiguration IP QoS Mode: None
*c xConfiguration IP QoS Value: 0
*c xConfiguration IP V6 Gateway: ""
*c xConfiguration IP DNS Domain Name: "#####.local"
*c xConfiguration IP DNS Hostname: "VCS1-Control"
*c xConfiguration IP Ephemeral PortRange Start: 40000
*c xConfiguration IP Ephemeral PortRange End: 49999
*c xConfiguration IP RFC4821 Mode: Disabled
*c xConfiguration Administration Telnet Mode: Off
*c xConfiguration Administration SSH Mode: On
*c xConfiguration Administration HTTP Mode: On
*c xConfiguration Administration HTTPS Mode: On
*c xConfiguration Administration LCDPanel Mode: On
*c xConfiguration ExternalManager Address: "10.10.10.104"
*c xConfiguration ExternalManager Path: "tms/public/external/management/system
managementservice.asmx"
*c xConfiguration ExternalManager Protocol: HTTP
*c xConfiguration ExternalManager Server Certificate Verification Mode: On
*c xConfiguration Registration RestrictionPolicy Mode: None
*c xConfiguration Registration RestrictionPolicy Service Protocol: HTTP
*c xConfiguration Registration RestrictionPolicy Service TLS Verify Mode: On
*c xConfiguration Registration RestrictionPolicy Service TLS CRLCheck Mode: Off
*c xConfiguration Registration RestrictionPolicy Service Server 1 Address: ""
*c xConfiguration Registration RestrictionPolicy Service Server 2 Address: ""
*c xConfiguration Registration RestrictionPolicy Service Server 3 Address: ""
*c xConfiguration Registration RestrictionPolicy Service Path: ""
*c xConfiguration Registration RestrictionPolicy Service Status Path: "status"
```

```
*c xConfiguration Registration RestrictionPolicy Service UserName: ""
*c xConfiguration Registration RestrictionPolicy Service Password: "{cipher}
XXXXXXXXXXXXXXXXXXXXXXXXXXXX"
*c xConfiguration Registration RestrictionPolicy Service DefaultCPL: "<reject
status='504' reason='Registration Policy Unavailable'/>"
*c xConfiguration Alternates ConfigurationMaster: 1
*c xConfiguration Alternates Cluster Name: ""
*c xConfiguration Alternates Peer 1 Address: ""
*c xConfiguration Alternates Peer 2 Address: ""
*c xConfiguration Alternates Peer 3 Address: ""
*c xConfiguration Alternates Peer 4 Address: ""
*c xConfiguration Alternates Peer 5 Address: ""
*c xConfiguration Alternates Peer 6 Address: ""
*c xConfiguration Transform 1 Description: "Transform destination aliases to
URI format"
*c xConfiguration Transform 1 State: Enabled
*c xConfiguration Transform 1 Priority: 1
*c xConfiguration Transform 1 Pattern String: "([^\@]*)"
*c xConfiguration Transform 1 Pattern Type: Regex
*c xConfiguration Transform 1 Pattern Behavior: Replace
*c xConfiguration Transform 1 Pattern Replace: "\1@#####.local"
*c xConfiguration Call Loop Detection Mode: On
*c xConfiguration Call Routed Mode: Always
*c xConfiguration Call Services CallsToUnknownIPAddresses: Indirect
*c xConfiguration Call Services Fallback Alias: ""
*c xConfiguration H323 Mode: On
*c xConfiguration H323 Gatekeeper Registration UDP Port: 1719
*c xConfiguration H323 Gatekeeper Registration ConflictMode: Reject
*c xConfiguration H323 Gatekeeper CallSignaling TCP Port: 1720
*c xConfiguration H323 Gatekeeper CallSignaling PortRange Start: 15000
*c xConfiguration H323 Gatekeeper CallSignaling PortRange End: 19999
*c xConfiguration H323 Gatekeeper TimeToLive: 1800
*c xConfiguration H323 Gatekeeper CallTimeToLive: 120
*c xConfiguration H323 Gatekeeper AutoDiscovery Mode: On
*c xConfiguration H323 Gateway CallerId: ExcludePrefix
*c xConfiguration SIP Mode: On
*c xConfiguration SIP Domains Domain 1 Name: "#####.com"
*c xConfiguration SIP Domains Domain 2 Name: "#####.local"
*c xConfiguration SIP Routes Route 1 Method: "SUBSCRIBE"
*c xConfiguration SIP Routes Route 1 Request Line Pattern: ".*@(%localdomains%|
%ip%)"
*c xConfiguration SIP Routes Route 1 Header Name: "Event"
*c xConfiguration SIP Routes Route 1 Header Pattern: "(ua-profile|phonebook).*"
*c xConfiguration SIP Routes Route 1 Authenticated: Off
*c xConfiguration SIP Routes Route 1 Address: "127.0.0.1"
*c xConfiguration SIP Routes Route 1 Port: 22400
*c xConfiguration SIP Routes Route 1 Transport: TCP
*c xConfiguration SIP Routes Route 1 Tag: "Provisioning"
*c xConfiguration SIP Routes Route 2 Method: "INFO"
*c xConfiguration SIP Routes Route 2 Request Line Pattern: ".*@(%localdomains%|
%ip%)"
*c xConfiguration SIP Routes Route 2 Header Name: "Content-Type"
*c xConfiguration SIP Routes Route 2 Header Pattern: "application/tandberg-
phonebook\+xml"
*c xConfiguration SIP Routes Route 2 Authenticated: Off
*c xConfiguration SIP Routes Route 2 Address: "127.0.0.1"
*c xConfiguration SIP Routes Route 2 Port: 22400
*c xConfiguration SIP Routes Route 2 Transport: TCP
*c xConfiguration SIP Routes Route 2 Tag: "Phonebook"
*c xConfiguration SIP Registration Standard Refresh Strategy: Maximum
*c xConfiguration SIP Registration Standard Refresh Minimum: 45
*c xConfiguration SIP Registration Standard Refresh Maximum: 60
*c xConfiguration SIP Registration Outbound Refresh Strategy: Variable
*c xConfiguration SIP Registration Outbound Refresh Minimum: 300
```

\*c xConfiguration SIP Registration Outbound Refresh Maximum: 3600  
\*c xConfiguration SIP Registration Outbound Flow Timer: 0  
\*c xConfiguration SIP Registration Proxy Mode: Off  
\*c xConfiguration SIP Registration Call Remove: No  
\*c xConfiguration SIP Session Refresh Value: 1800  
\*c xConfiguration SIP Session Refresh Minimum: 500  
\*c xConfiguration SIP UDP Mode: Off  
\*c xConfiguration SIP UDP Port: 5060  
\*c xConfiguration SIP TCP Mode: On  
\*c xConfiguration SIP TCP Port: 5060  
\*c xConfiguration SIP TCP Outbound Port Start: 25000  
\*c xConfiguration SIP TCP Outbound Port End: 29999  
\*c xConfiguration SIP TLS Mode: On  
\*c xConfiguration SIP TLS Port: 5061  
\*c xConfiguration SIP TLS Certificate Revocation Checking Mode: Off  
\*c xConfiguration SIP TLS Certificate Revocation Checking OCSP Mode: On  
\*c xConfiguration SIP TLS Certificate Revocation Checking CRL Mode: On  
\*c xConfiguration SIP TLS Certificate Revocation Checking CRL Network Fetch  
Mode: On  
\*c xConfiguration SIP TLS Certificate Revocation Checking Source Inaccessibility  
Behavior: Fail  
\*c xConfiguration SIP Require UDP BFCP Mode: On  
\*c xConfiguration SIP Require Duo Video Mode: On  
\*c xConfiguration SIP Authentication Retry Limit: 3  
\*c xConfiguration SIP Authentication NTLM Mode: Auto  
\*c xConfiguration SIP Authentication NTLM SA Lifetime: 28800  
\*c xConfiguration SIP Authentication NTLM SA Limit: 10000  
\*c xConfiguration SIP Authentication Digest Nonce ExpireDelta: 300  
\*c xConfiguration SIP Authentication Digest Nonce Maximum Use Count: 128  
\*c xConfiguration SIP Authentication Digest Nonce Limit: 10000  
\*c xConfiguration SIP Authentication Digest Nonce Length: 60  
\*c xConfiguration SIP GRUU Mode: On  
\*c xConfiguration SIP MediaRouting ICE Mode: Off  
\*c xConfiguration Interworking Mode: RegisteredOnly  
\*c xConfiguration Interworking Encryption Mode: Auto  
\*c xConfiguration Interworking Encryption Replay Protection Mode: Off  
\*c xConfiguration Interworking BFCP Compatibility Mode: Auto  
\*c xConfiguration Interworking Require Invite Header Mode: On  
\*c xConfiguration Traversal Media Port Start: 50000  
\*c xConfiguration Traversal Media Port End: 52399  
\*c xConfiguration Authentication UserName: ""  
\*c xConfiguration Authentication Password: "{cipher}XXXXXXXXXXXXXXXXXXXXXXXXXX"  
\*c xConfiguration Authentication LDAP AliasOrigin: LDAP  
\*c xConfiguration Authentication ADS ADDomain: ""  
\*c xConfiguration Authentication ADS Workgroup: ""  
\*c xConfiguration Authentication ADS MachinePassword Refresh: On  
\*c xConfiguration Authentication ADS SPNEGO: Enabled  
\*c xConfiguration Authentication ADS SecureChannel: Auto  
\*c xConfiguration Authentication ADS Encryption: TLS  
\*c xConfiguration Authentication ADS Mode: Off  
\*c xConfiguration Authentication ADS Clockskew: 300  
\*c xConfiguration Zones Policy Mode: SearchRules  
\*c xConfiguration Zones Policy SearchRules Rule 1 Name: "Local zone ? no domain"  
\*c xConfiguration Zones Policy SearchRules Rule 1 Description: "Search local  
zone for H.323 devices (strip domain)"  
\*c xConfiguration Zones Policy SearchRules Rule 1 Priority: 48  
\*c xConfiguration Zones Policy SearchRules Rule 1 Protocol: Any  
\*c xConfiguration Zones Policy SearchRules Rule 1 Source Mode: Any  
\*c xConfiguration Zones Policy SearchRules Rule 1 Authentication: No  
\*c xConfiguration Zones Policy SearchRules Rule 1 Mode: AliasPatternMatch  
\*c xConfiguration Zones Policy SearchRules Rule 1 Pattern Type: Regex  
\*c xConfiguration Zones Policy SearchRules Rule 1 Pattern String: "(.+)@#####.local.\*"  
\*c xConfiguration Zones Policy SearchRules Rule 1 Pattern Behavior: Replace

```

*c xConfiguration Zones Policy SearchRules Rule 1 Pattern Replace: "\1"
*c xConfiguration Zones Policy SearchRules Rule 1 Progress: Continue
*c xConfiguration Zones Policy SearchRules Rule 1 Target Type: Zone
*c xConfiguration Zones Policy SearchRules Rule 1 Target Name: "LocalZone"
*c xConfiguration Zones Policy SearchRules Rule 1 State: Enabled
*c xConfiguration Zones Policy SearchRules Rule 2 Name: "Local zone ? full URI"
*c xConfiguration Zones Policy SearchRules Rule 2 Description: "Search local
zone for SIP and H.323 devices with a domain"
*c xConfiguration Zones Policy SearchRules Rule 2 Priority: 51
*c xConfiguration Zones Policy SearchRules Rule 2 Protocol: Any
*c xConfiguration Zones Policy SearchRules Rule 2 Source Mode: Any
*c xConfiguration Zones Policy SearchRules Rule 2 Authentication: No
*c xConfiguration Zones Policy SearchRules Rule 2 Mode: AliasPatternMatch
*c xConfiguration Zones Policy SearchRules Rule 2 Pattern Type: Regex
*c xConfiguration Zones Policy SearchRules Rule 2 Pattern String: "(.+
@#####.local.*"
*c xConfiguration Zones Policy SearchRules Rule 2 Pattern Behavior: Leave
*c xConfiguration Zones Policy SearchRules Rule 2 Pattern Replace: ""
*c xConfiguration Zones Policy SearchRules Rule 2 Progress: Continue
*c xConfiguration Zones Policy SearchRules Rule 2 Target Type: Zone
*c xConfiguration Zones Policy SearchRules Rule 2 Target Name: "LocalZone"
*c xConfiguration Zones Policy SearchRules Rule 2 State: Enabled
*c xConfiguration Zones Policy SearchRules Rule 3 Name: "Traversal zone search rule"
*c xConfiguration Zones Policy SearchRules Rule 3 Description: "Search traversal
zone (Cisco VCS Expressway)"
*c xConfiguration Zones Policy SearchRules Rule 3 Priority: 100
*c xConfiguration Zones Policy SearchRules Rule 3 Protocol: Any
*c xConfiguration Zones Policy SearchRules Rule 3 Source Mode: Any
*c xConfiguration Zones Policy SearchRules Rule 3 Authentication: No
*c xConfiguration Zones Policy SearchRules Rule 3 Mode: AnyAlias
*c xConfiguration Zones Policy SearchRules Rule 3 Progress: Continue
*c xConfiguration Zones Policy SearchRules Rule 3 Target Type: Zone
*c xConfiguration Zones Policy SearchRules Rule 3 Target Name: "TraversalZone"
*c xConfiguration Zones Policy SearchRules Rule 3 State: Enabled
*c xConfiguration Zones Policy SearchRules Rule 4 Name: "External IP address
search rule"
*c xConfiguration Zones Policy SearchRules Rule 4 Description: "Route external
IP address"
*c xConfiguration Zones Policy SearchRules Rule 4 Priority: 100
*c xConfiguration Zones Policy SearchRules Rule 4 Protocol: Any
*c xConfiguration Zones Policy SearchRules Rule 4 Source Mode: Any
*c xConfiguration Zones Policy SearchRules Rule 4 Authentication: No
*c xConfiguration Zones Policy SearchRules Rule 4 Mode: AnyIPAddress
*c xConfiguration Zones Policy SearchRules Rule 4 Progress: Continue
*c xConfiguration Zones Policy SearchRules Rule 4 Target Type: Zone
*c xConfiguration Zones Policy SearchRules Rule 4 Target Name: "TraversalZone"
*c xConfiguration Zones Policy SearchRules Rule 4 State: Enabled
*c xConfiguration Zones Policy SearchRules Rule 5 Name: "LocalZoneMatch"
*c xConfiguration Zones Policy SearchRules Rule 5 Description: "Default rule:
queries the Local Zone for any alias"
*c xConfiguration Zones Policy SearchRules Rule 5 Priority: 50
*c xConfiguration Zones Policy SearchRules Rule 5 Protocol: Any
*c xConfiguration Zones Policy SearchRules Rule 5 Source Mode: Any
*c xConfiguration Zones Policy SearchRules Rule 5 Authentication: No
*c xConfiguration Zones Policy SearchRules Rule 5 Mode: AnyAlias
*c xConfiguration Zones Policy SearchRules Rule 5 Progress: Continue
*c xConfiguration Zones Policy SearchRules Rule 5 Target Type: Zone
*c xConfiguration Zones Policy SearchRules Rule 5 Target Name: "LocalZone"
*c xConfiguration Zones Policy SearchRules Rule 5 State: Enabled
*c xConfiguration Zones DefaultZone Authentication Mode: DoNotCheckCredentials
*c xConfiguration Zones DefaultZone SIP Record Route Address Type: IP
*c xConfiguration Zones DefaultZone SIP TLS Verify Mode: Off
*c xConfiguration Zones DefaultZone SIP Media Encryption Mode: Auto
*c xConfiguration Zones LocalZone DefaultSubZone SIP Media Encryption Mode: Auto

```



```
*c xConfiguration Zones LocalZone DefaultSubZone Authentication Mode:
DoNotCheckCredentials
*c xConfiguration Zones LocalZone DefaultSubZone Registrations: Allow
*c xConfiguration Zones LocalZone DefaultSubZone Bandwidth Total Mode: Unlimited
*c xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Inter Mode:
Unlimited
*c xConfiguration Zones LocalZone DefaultSubZone Bandwidth PerCall Intra Mode:
Unlimited
*c xConfiguration Zones LocalZone TraversalSubZone Bandwidth Total Mode: Unlimited
*c xConfiguration Zones LocalZone TraversalSubZone Bandwidth PerCall Mode:
Unlimited
*c xConfiguration Zones LocalZone SIP Record Route Address Type: IP
*c xConfiguration Zones Zone 1 Name: "TraversalZone"
*c xConfiguration Zones Zone 1 HopCount: 15
*c xConfiguration Zones Zone 1 H323 Mode: On
*c xConfiguration Zones Zone 1 SIP Mode: On
*c xConfiguration Zones Zone 1 Type: TraversalClient
*c xConfiguration Zones Zone 1 TraversalClient Authentication Mode: DoNot
CheckCredentials
*c xConfiguration Zones Zone 1 TraversalClient Authentication UserName:
"#####auth"
*c xConfiguration Zones Zone 1 TraversalClient Authentication Password:
"{cipher}XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
*c xConfiguration Zones Zone 1 TraversalClient Registrations: Allow
*c xConfiguration Zones Zone 1 TraversalClient H323 Protocol: Assent
*c xConfiguration Zones Zone 1 TraversalClient H323 Port: 6001
*c xConfiguration Zones Zone 1 TraversalClient SIP Protocol: Assent
*c xConfiguration Zones Zone 1 TraversalClient SIP Port: 7001
*c xConfiguration Zones Zone 1 TraversalClient SIP Transport: TLS
*c xConfiguration Zones Zone 1 TraversalClient SIP TLS Verify Mode: Off
*c xConfiguration Zones Zone 1 TraversalClient SIP Poison Mode: Off
*c xConfiguration Zones Zone 1 TraversalClient SIP Media Encryption Mode: Auto
*c xConfiguration Zones Zone 1 TraversalClient RetryInterval: 120
*c xConfiguration Zones Zone 1 TraversalClient Peer 1 Address: "10.10.10.102"
*c xConfiguration Zones Zone 1 TraversalClient Peer 2 Address: ""
*c xConfiguration Zones Zone 1 TraversalClient Peer 3 Address: ""
*c xConfiguration Zones Zone 1 TraversalClient Peer 4 Address: ""
*c xConfiguration Zones Zone 1 TraversalClient Peer 5 Address: ""
*c xConfiguration Zones Zone 1 TraversalClient Peer 6 Address: ""
*c xConfiguration Bandwidth Default: 384
*c xConfiguration Bandwidth Downspeed PerCall Mode: On
*c xConfiguration Bandwidth Downspeed Total Mode: On
*c xConfiguration Bandwidth Link 1 Name: "DefaultSZtoTraversalSZ"
*c xConfiguration Bandwidth Link 1 Node1 Name: "DefaultSubZone"
*c xConfiguration Bandwidth Link 1 Node2 Name: "TraversalSubZone"
*c xConfiguration Bandwidth Link 1 Pipe1 Name: ""
*c xConfiguration Bandwidth Link 1 Pipe2 Name: ""
*c xConfiguration Bandwidth Link 2 Name: "DefaultSZtoDefaultZ"
*c xConfiguration Bandwidth Link 2 Node1 Name: "DefaultSubZone"
*c xConfiguration Bandwidth Link 2 Node2 Name: "DefaultZone"
*c xConfiguration Bandwidth Link 2 Pipe1 Name: ""
*c xConfiguration Bandwidth Link 2 Pipe2 Name: ""
*c xConfiguration Bandwidth Link 3 Name: "DefaultSZtoClusterSZ"
*c xConfiguration Bandwidth Link 3 Node1 Name: "DefaultSubZone"
*c xConfiguration Bandwidth Link 3 Node2 Name: "ClusterSubZone"
*c xConfiguration Bandwidth Link 3 Pipe1 Name: ""
*c xConfiguration Bandwidth Link 3 Pipe2 Name: ""
*c xConfiguration Bandwidth Link 4 Name: "TraversalSZtoDefaultZ"
*c xConfiguration Bandwidth Link 4 Node1 Name: "TraversalSubZone"
*c xConfiguration Bandwidth Link 4 Node2 Name: "DefaultZone"
*c xConfiguration Bandwidth Link 4 Pipe1 Name: ""
*c xConfiguration Bandwidth Link 4 Pipe2 Name: ""
*c xConfiguration Bandwidth Link 5 Name: "Zone001ToTraversalSZ"
*c xConfiguration Bandwidth Link 5 Node1 Name: "TraversalZone"
```

```
*c xConfiguration Bandwidth Link 5 Node2 Name: "TraversalSubZone"
*c xConfiguration Bandwidth Link 5 Pipe1 Name: ""
*c xConfiguration Bandwidth Link 5 Pipe2 Name: ""
*c xConfiguration Policy AdministratorPolicy Mode: Off
*c xConfiguration Policy AdministratorPolicy Service Protocol: HTTP
*c xConfiguration Policy AdministratorPolicy Service TLS Verify Mode: On
*c xConfiguration Policy AdministratorPolicy Service TLS CRLCheck Mode: Off
*c xConfiguration Policy AdministratorPolicy Service Server 1 Address: ""
*c xConfiguration Policy AdministratorPolicy Service Server 2 Address: ""
*c xConfiguration Policy AdministratorPolicy Service Server 3 Address: ""
*c xConfiguration Policy AdministratorPolicy Service Path: ""
*c xConfiguration Policy AdministratorPolicy Service Status Path: "status"
*c xConfiguration Policy AdministratorPolicy Service UserName: ""
*c xConfiguration Policy AdministratorPolicy Service Password: "{cipher}
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX"
*c xConfiguration Policy AdministratorPolicy Service DefaultCPL: "<reject
status='504' reason='Admin Policy Unavailable'/">"
*c xConfiguration Policy FindMe Mode: Off
*c xConfiguration Policy FindMe CallerId: IncomingID
*c xConfiguration Policy FindMe UserDeviceRestriction: Off
*c xConfiguration Applications ConferenceFactory Mode: Off
*c xConfiguration Applications ConferenceFactory Alias: ""
*c xConfiguration Applications ConferenceFactory Template: ""
*c xConfiguration Applications ConferenceFactory Range Start: 1
*c xConfiguration Applications ConferenceFactory Range End: 65535
*c xConfiguration Applications OCS Relay Mode: Off
*c xConfiguration Applications OCS Relay OCS Domain: ""
*c xConfiguration Applications OCS Relay OCS Routing Prefix: "ocs"
*c xConfiguration Applications Presence Server Mode: Off
*c xConfiguration Applications Presence Server Publication ExpireDelta: 1800
*c xConfiguration Applications Presence Server Subscription ExpireDelta: 3600
*c xConfiguration Applications Presence User Agent Mode: Off
*c xConfiguration Applications Presence User Agent ExpireDelta: 3600
*c xConfiguration Applications Presence User Agent RetryDelta: 1800
*c xConfiguration Applications Presence User Agent Presentity Idle Status: Online
*c xConfiguration ResourceUsage Warning Activation Level: 90
*c xConfiguration Services AdvancedMediaGateway Zone Name: ""
*c xConfiguration Services AdvancedMediaGateway Policy Mode: Off
```

```
OK
exit
Bye!
```

## Risoluzione dei problemi

Di seguito sono riportati i tre problemi più comuni che possono verificarsi:

- **Il cavo seriale utilizzato non è corretto o è difettoso.** Assicurarsi di utilizzare il cavo fornito con il dispositivo.
- **I caratteri non riconoscibili vengono visualizzati sullo schermo della console.** Ciò indica che la velocità in baud non è impostata correttamente. Le velocità in baud si basano su multipli di due, quindi è possibile raddoppiare o dimezzare il valore in base alle esigenze fino a trovare l'impostazione corretta. In questo caso, l'impostazione corretta dovrebbe essere **115.200**.
- **Non è possibile connettersi al software di emulazione del terminale.** Oltre ai problemi relativi al cablaggio, questo problema è in genere causato da uno dei seguenti problemi:

Quando si tenta di connettersi tramite Telnet o SSH, è necessario impostare il tipo di connessione su seriale quando si utilizza una connessione seriale.

Porta COM non corretta. Per individuare la porta COM utilizzata dal PC con connessioni seriali basate su USB, selezionare **Pannello di controllo > Gestione dispositivi**, quindi fare clic su **Porte**. Da questa finestra è possibile verificare la porta COM assegnata al dispositivo seriale USB.

Non sono installati i driver per il dispositivo seriale. In questo caso, è necessario individuarli e installarli.

- **Non è possibile accedere al protocollo SSH nel dispositivo.** Oltre ai problemi relativi al cablaggio, questo problema è in genere causato da uno dei seguenti problemi:

Si è tentato di connettersi tramite SSH e il dispositivo non è raggiungibile a causa di problemi di connettività di rete. Risolvere il problema di connettività di rete. In alternativa, è possibile che il protocollo SSH non sia abilitato per il dispositivo. Collegare il Web/HTTP/HTTPS al dispositivo e verificare che l'accesso SSH sia abilitato in:

**Configuration>SystemConfiguration>Network Services.**

Non si dispone di una chiave Rivest-Shamir-Addleman (RSA) memorizzata nella cache del dispositivo. In genere viene richiesto di accettare la chiave RSA. Accertarsi di accettare la chiave.

L'accesso non è riuscito a causa di un nome utente e di una password errati. Accertarsi di utilizzare il nome utente e la password corretti per il dispositivo.