

VCS Series ou Expressway Series Xconfig e Xstatus Output Collection com PuTTY

Contents

[Introduction](#)

[Prerequisites](#)

[Requirements](#)

[Componentes Utilizados](#)

[Configurar](#)

[Conectar por console](#)

[Conectar via SSH](#)

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

[Verificar](#)

[Troubleshoot](#)

Introduction

Este documento descreve como coletar a saída CLI dos comandos **xconfig** e **xstatus** da série VCS (Video Communication Server) e Expressway Series dos dispositivos VCS-Control, VCS-Expressway, Expressway-C e Expressway-E, que o Cisco Technical Assistance Center (TAC) ocasionalmente precisa recuperar.

Prerequisites

Requirements

A Cisco recomenda que você tenha conhecimento destes tópicos:

- PuTTY ou software de emulação de terminal semelhante, como SecureCRT, Tera Term ou similar.
- Nome de usuário e senha da conta do administrador para o dispositivo da série VCS/Expressway.
- Cabo de console serial RJ45-D-Sub9pin ou Shell seguro (SSH) permitido no caminho da rede.

Componentes Utilizados

As informações neste documento são baseadas nestas versões de software e hardware:

- PuTTY (Visite a [página de download PuTTY](#) para obter uma cópia).
- Um VCS-C que executa a versão 7.2.1 é usado neste exemplo, que é aplicável através da versão 8.2.2, que é a versão mais recente no momento.

Configurar

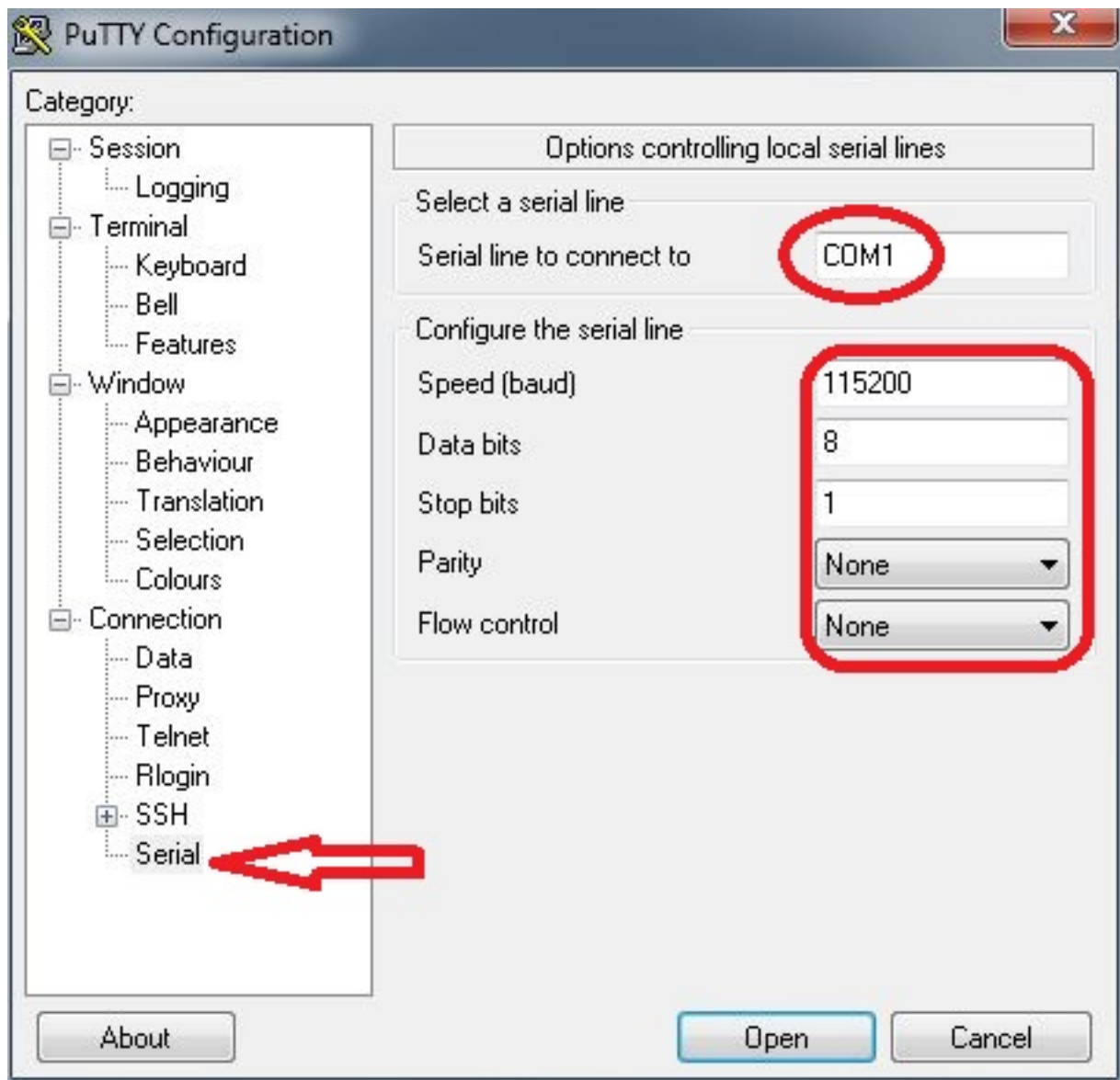
Conectar por console

Note: Este artigo pressupõe que você tenha um cabo de console serial físico funcional conectado. Você deve ter recebido um com seu dispositivo.

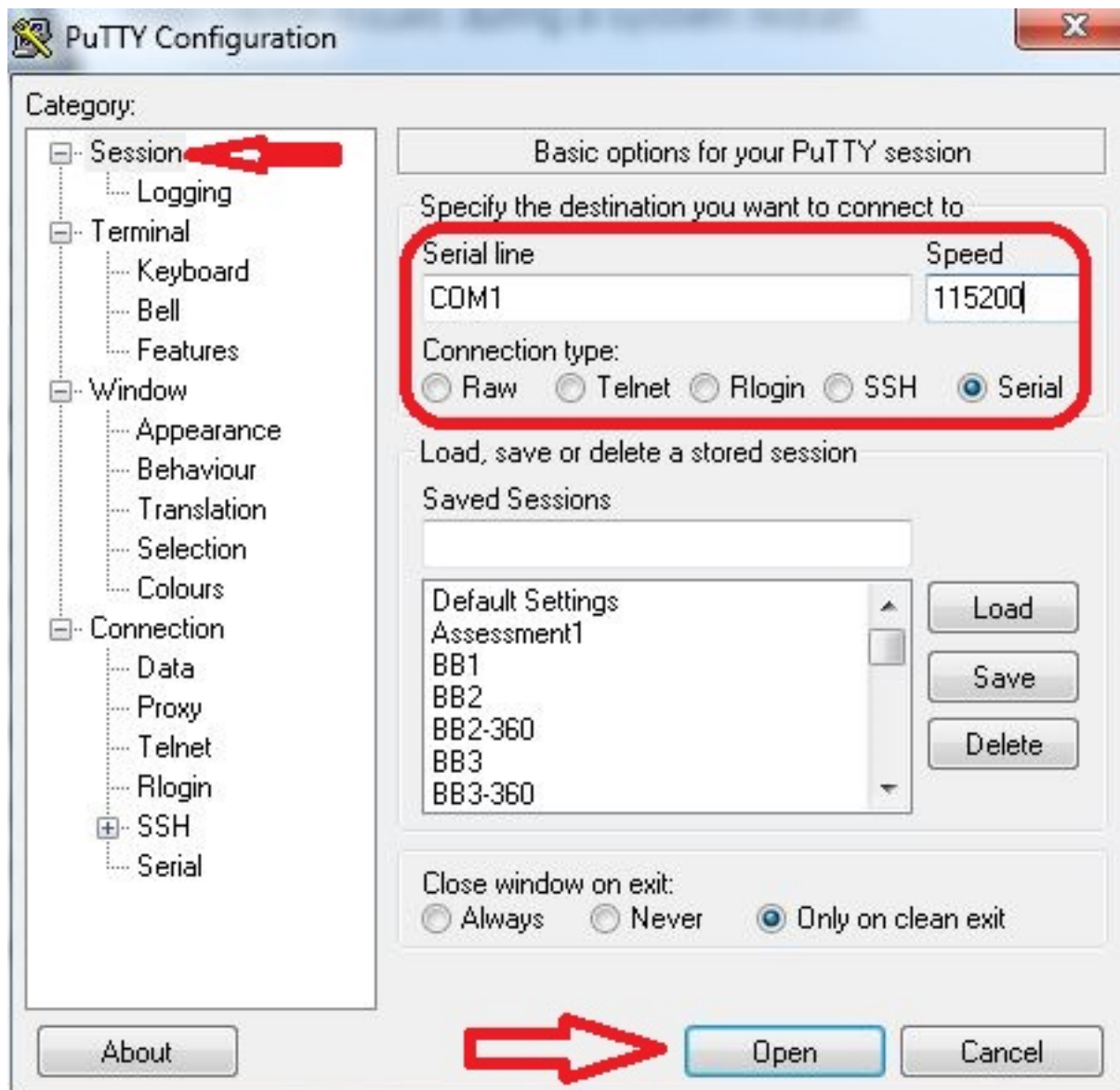
Aqui está um exemplo das configurações que você deve configurar para acesso de console serial em PuTTY.

Note: Você precisará ajustar a porta Comunicação (COM) com base na forma como o console está conectado ao seu PC.

1. Vá para **Configuration > Category > Connection > Serial** e ajuste as configurações seriais conforme mostrado aqui:



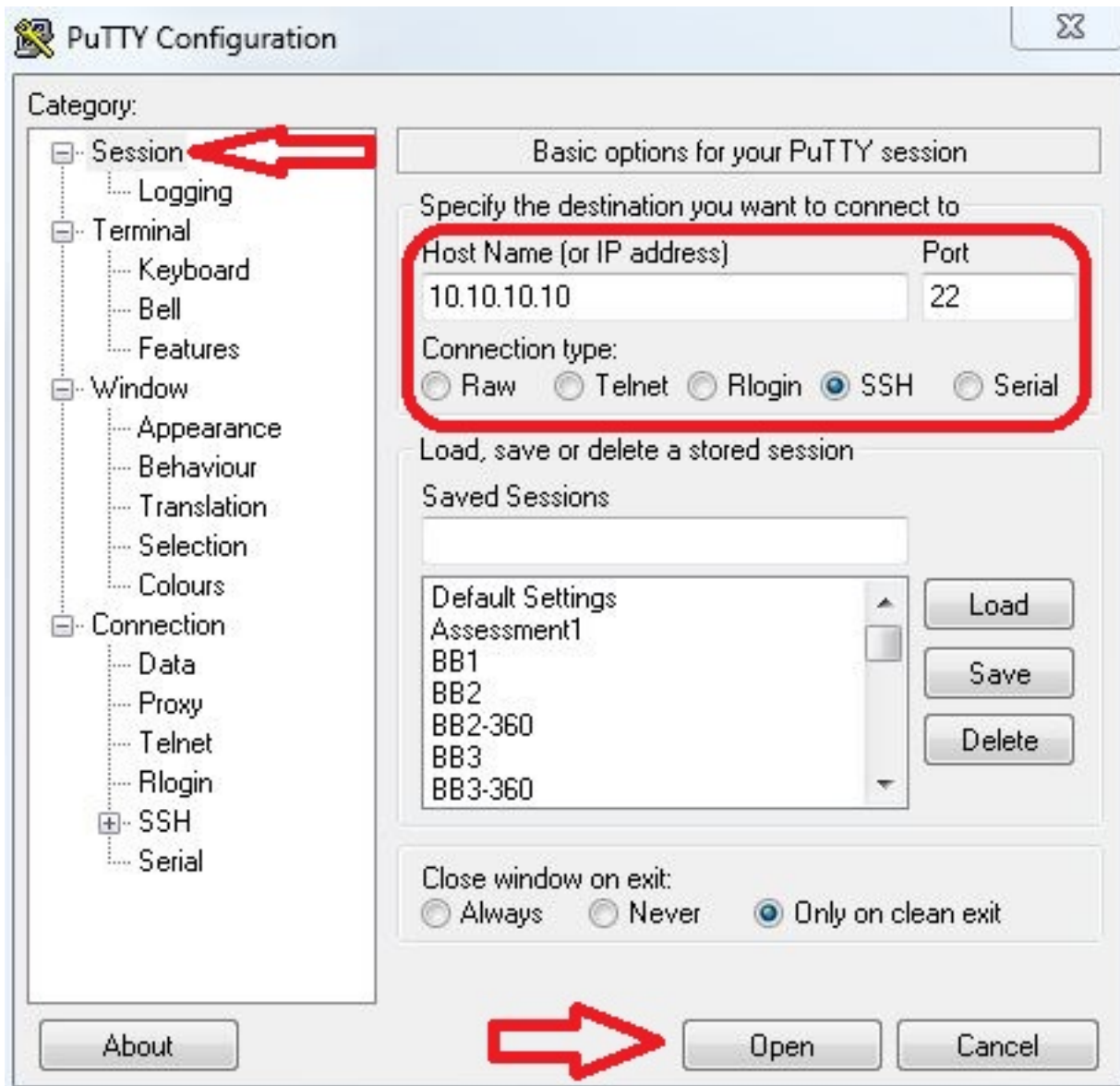
2. Vá para **Categoria > Sessão**, selecione **Tipo de série** como o tipo de conexão e clique em **Abrir** como mostrado aqui:



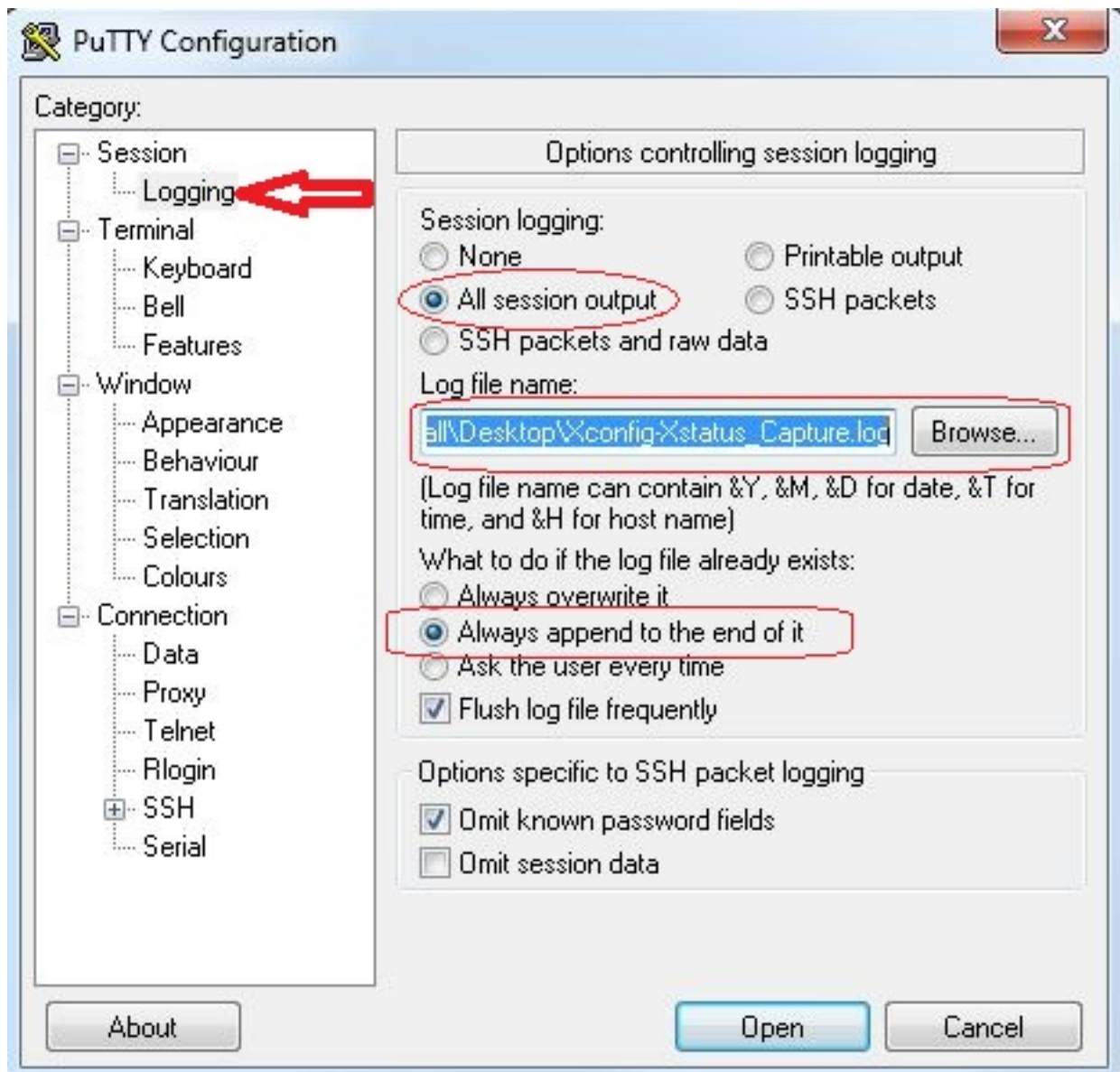
Conectar via SSH

Uma alternativa mais simples é o SSH no dispositivo.

1. Use o endereço IP do seu dispositivo VCS/Expressway para ajustar suas configurações em PuTTY, como mostrado neste exemplo:



2. Antes ou durante a sessão PuTTY no dispositivo, você deve definir as Configurações de registro. Para fazer isso, vá para **Configuration > Category > Session > Logging** e configure as configurações de acordo com este exemplo (ajuste o caminho do arquivo e o nome do arquivo de acordo com seu PC e suas necessidades):



3. Quando conectado e conectado, uma tela semelhante a esta é exibida. Faça login como admin, conforme indicado aqui.

```
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
```

Caution: Como este é um ambiente de laboratório, os alarmes podem ser ignorados. Se os alarmes forem vistos em um ambiente de produção, eles devem ser abordados o mais rápido possível.

4. Digite o comando `xstatus` e pressione **Enter**:

```
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

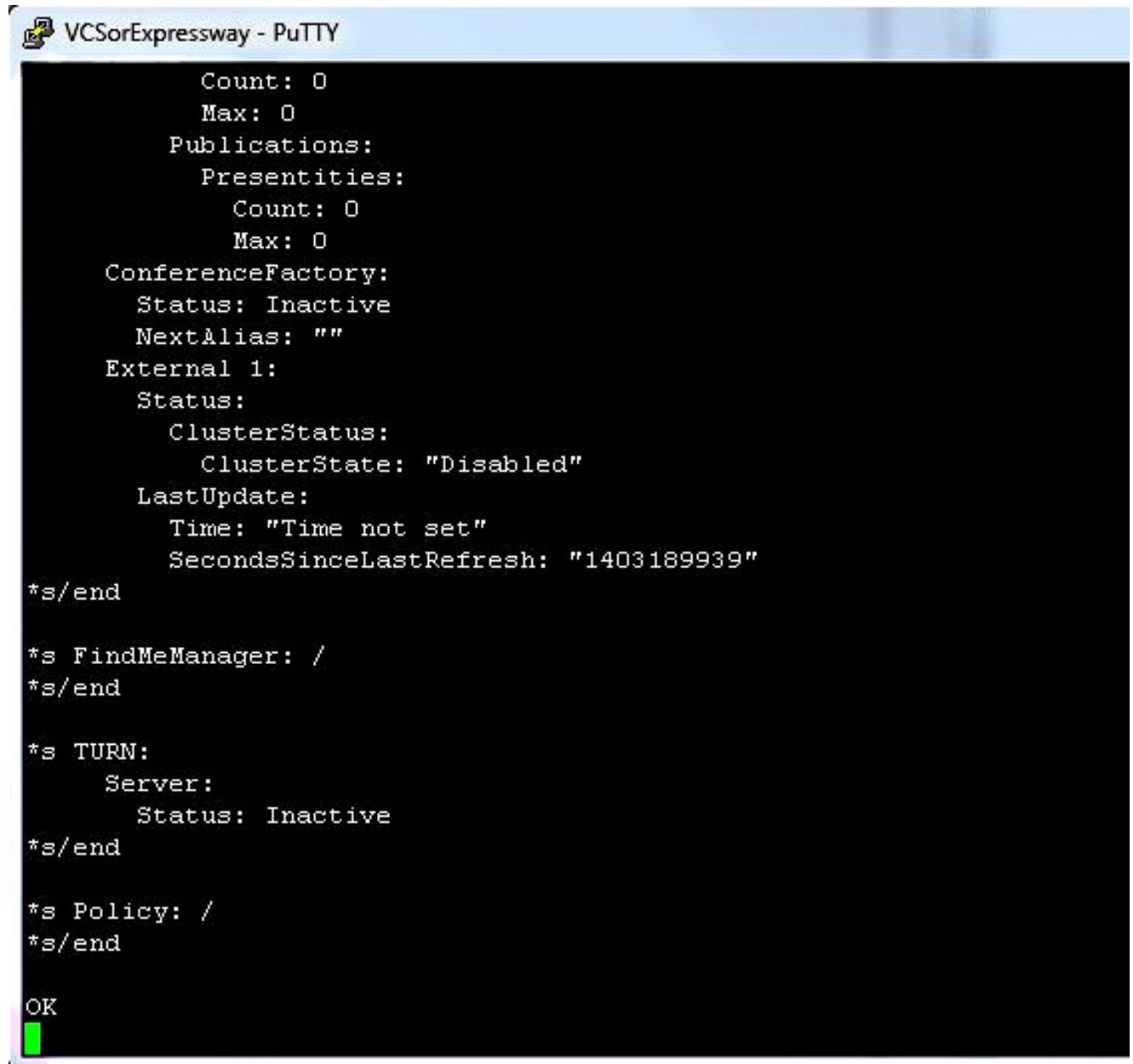
Last login: Thu Jun 19 08:12:21 EDT 2014
Welcome to VCS1-Control
TANDBERG VCS Release X7.2.1
SW Release Date: 2012-09-25

OK

xstatus
```

Esta é a saída `xstatus` exibida após você pressionar **Enter**. A saída rolou muito rapidamente

para visualizar até o final. Desde que o registro tenha sido configurado anteriormente, ele estará no arquivo de texto.



```
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
```

Agora que você coletou a saída do comando **xstatus**, você está pronto para coletar a saída do comando **xconfig**.

5. Digite o comando **xconfig** e pressione **Enter**.


```
xconfig █
```

Aqui está um exemplo da saída **xconfig** depois de pressionar enter. A saída rolou muito rapidamente para visualizar até o final. Desde que o registro tenha sido configurado anteriormente, ele estará no arquivo de texto.

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

VCS e Expressway Series x8.2

Na versão de software do x8.2, o `xconfiguration` e o `xstatus` são agora incluídos quando um log de diagnóstico é realizado.

1. Vá para **Manutenção > Diagnóstico > Log de diagnóstico**.
2. Selecione **Iniciar novo log** e, em seguida, **Parar registro** imediatamente.

Note: Este método também contém o `logging_snapshot.txt` que registra mensagens em resposta às atividades que ocorrem no VCS ou na Série Expressway no momento.

O arquivo de log de diagnóstico baixado contém estes arquivos:

`loggingsnapshot.txt` - Contém mensagens de log em resposta às atividades executadas durante o período de log.

`xconf_dump.txt` - Contém informações sobre a configuração do sistema no momento em que o registro foi iniciado.

`xstat_dump.txt` - Contém informações sobre o status do sistema no momento em que o registro foi iniciado.

(se relevante) `diagnostic_logging_tcpdump.pcap` - Contém os pacotes capturados durante o período de registro.

Verificar

Aqui está um exemplo de como a saída **xstatus** e **xconfig** se parece no arquivo de texto salvo com as configurações de registro:

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}
XXXXXXXXXXXXXXXXXXXXXXXXXX"
*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!

```

Troubleshoot

Estes são os três problemas mais comuns que você pode encontrar:

- **Um cabo serial incorreto ou defeituoso é usado.** Certifique-se de usar o cabo fornecido com o dispositivo.
- **Caracteres não reconhecíveis são exibidos na tela do console.** Isso indica que a taxa de baud está definida incorretamente. As taxas de baud são baseadas em múltiplos de dois, de modo que você pode dobrar ou reduzir para metade o valor conforme necessário até encontrar a configuração correta. Nesse caso, a configuração correta deve ser **115.200**.
- **Você não pode se conectar ao software de emulação de terminal.** Além dos problemas de cabeamento, esse problema é normalmente causado por um destes problemas:

Você tenta se conectar via Telnet ou SSH e deve alterar seu tipo de conexão para serial quando usa uma conexão serial.

Você está na porta COM incorreta. Para descobrir a porta COM que o PC usa com conexões seriais baseadas em USB, navegue até **Painel de controle > Gerenciador de dispositivos** e clique em **Portas**. Nessa janela, você pode verificar a porta COM atribuída ao dispositivo serial USB.

Você não tem os drivers do dispositivo serial instalados. Se esse for o caso, você deve localizá-los e instalá-los.

- **Não é possível executar SSH no dispositivo.** Além dos problemas de cabeamento, esse problema é normalmente causado por um destes problemas:

Você tenta se conectar via SSH e não consegue acessar o dispositivo devido a problemas de conectividade de rede. Corrija o problema de conectividade de rede. Como alternativa, o SSH pode não estar ativado para o dispositivo. Web/HTTP/HTTPS no dispositivo e verifique se o acesso SSH está habilitado em: **Configuration>SystemConfiguration>Network Services**.

Você não tem uma chave Rivest-Shamir-Addleman (RSA) armazenada em cache no dispositivo. Normalmente, você é solicitado a aceitar a chave RSA. Assegure-se de aceitar a chave.

Seu login falha devido a um nome de usuário e uma senha incorretos. Certifique-se de usar o nome de usuário e a senha corretos para o dispositivo.