

# Configurazione dell'accesso remoto e mobile tramite Expressway/VCS in un'installazione multidominio

## Sommario

[Introduzione](#)

[Prerequisiti](#)

[Requisiti](#)

[Componenti usati](#)

[Configurazione](#)

[Esempio di rete](#)

[Zona trasversale](#)

[Traversal Server](#)

[Client trasversale](#)

[Dominio servizi voce](#)

[Record DNS](#)

[Domini SIP su Expressway-C](#)

[Nome host/Indirizzo IP server CUCM](#)

[Certificati](#)

[Doppia NIC](#)

[Due interfacce](#)

[One Interface - Indirizzo IP pubblico](#)

[One Interface - Indirizzo IP privato](#)

[Verifica](#)

[Risoluzione dei problemi](#)

[Zona trasversale](#)

[Doppia NIC](#)

[DNS](#)

[Domini SIP](#)

## Introduzione

Questo documento descrive come configurare Cisco TelePresence Video Communication Server (VCS) per Mobile Remote Access (MRA) quando si usano più domini.

La configurazione dell'MRA quando è presente un solo dominio è relativamente semplice ed è possibile seguire i passaggi descritti nella guida alla distribuzione. Quando la distribuzione coinvolge più domini, diventa più complessa. Questo documento non è una guida alla configurazione, ma descrive gli aspetti importanti quando sono coinvolti più domini. La configurazione principale è documentata nella [Guida all'implementazione di Cisco TelePresence Video Communication Server \(VCS\)](#).

# Prerequisiti

## Requisiti

Nessun requisito specifico previsto per questo documento.

## Componenti usati

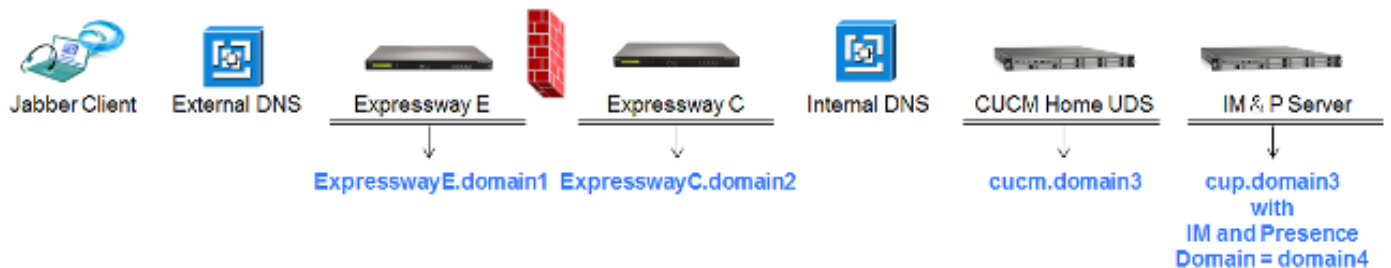
Il documento può essere consultato per tutte le versioni software o hardware.

Le informazioni discusse in questo documento fanno riferimento a dispositivi usati in uno specifico ambiente di emulazione. Su tutti i dispositivi menzionati nel documento la configurazione è stata ripristinata ai valori predefiniti. Se la rete è operativa, valutare attentamente eventuali conseguenze derivanti dall'uso dei comandi.

# Configurazione

Per configurare il software VCS, attenersi alle informazioni descritte in questa sezione.

## Esempio di rete

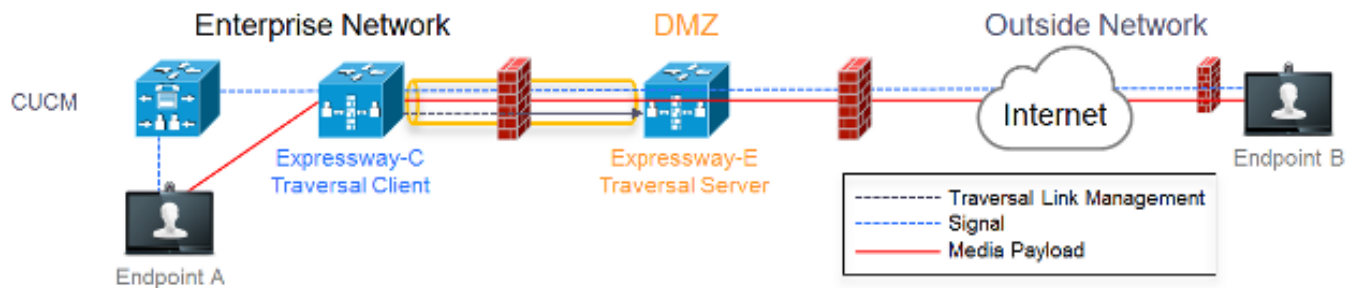


Di seguito è riportata una breve panoramica dei diversi domini:

- **dominio1**: dominio di Edge utilizzato dal client per individuare la posizione del server Edge e attraverso il quale viene rilevato il servizio User Data Service (UDS).
- **domain2 e domain3** - Utilizzato per l'individuazione dei server.
- **domain4** - Dominio di messaggistica immediata e presenza (IM&P) utilizzato dal traffico XCP (Extensible Communications Platform) e XMPP (Extensible Messaging and Presence Protocol).

## Zona trasversale

La zona trasversale è costituita dal server trasversale (**expresswayE**), situato nella zona demilitarizzata (DMZ), e dal client trasversale (**expresswayC**), situato all'interno della rete:



## Traversal Server

Traversal Server si trova nella configurazione della zona su Expressway E:

<p><b>Configuration</b></p> <p>Name: <input type="text" value="TraversalZone"/></p> <p>Type: <input type="text" value="Traversal server"/></p> <p>Hop count: <input type="text" value="15"/></p>	<p>Select type as Traversal Server</p>
<p><b>Connection credentials</b></p> <p>Username: <input type="text" value="traversal"/></p> <p>Password: <a href="#">Add/Edit local authentication database</a></p>	<p>Configure username for Traversal Client to authenticate with with server</p>
<p><b>H.323</b></p> <p>Mode: <input type="text" value="Off"/></p> <p>Protocol: <input type="text" value="Assent"/></p> <p>H.460.19 demultiplexing mode: <input type="text" value="Off"/></p>	<p>H.323 Mode must be set to off</p>
<p><b>SIP</b></p> <p>Mode: <input type="text" value="On"/></p> <p>Port: <input type="text" value="7001"/></p> <p>Transport: <input type="text" value="TLS"/></p> <p>Unified Communications services: <input type="text" value="Yes"/></p> <p>TLS verify mode: <input type="text" value="On"/></p> <p>TLS verify subject name: <input type="text" value="expresswayc.vnglp.lab"/></p> <p>Media encryption mode: <input type="text" value="Force encrypted"/></p> <p>ICE support: <input type="text" value="Off"/></p> <p>Poison mode: <input type="text" value="Off"/></p>	<p>Port 7001 is default listening port for Traversal Client connection</p>
<p><b>Authentication</b></p> <p>Authentication policy: <input type="text" value="Do not check credentials"/></p>	<p>Must be set to 'Do not check credentials' as expressway does not register any endpoints</p>

## Client trasversale

Traversal Client si trova nella configurazione della zona su Expressway C:

<p><b>Configuration</b></p> <p>Name <input type="text" value="TraversalZone"/></p> <p>Type <input type="text" value="Traversal client"/></p> <p>Hop count <input type="text" value="15"/></p>	Select Traversal Client as Type
<p><b>Connection credentials</b></p> <p>Username <input type="text" value="traversal"/></p> <p>Password <input type="password" value="*****"/></p>	Configure same username and password as added on the Traversal Server (Expressway E)
<p><b>H.323</b></p> <p>Mode <input type="text" value="Off"/></p> <p>Protocol <input type="text" value="Assent"/></p>	H.323 mode must be set to off
<p><b>SIP</b></p> <p>Mode <input type="text" value="On"/></p> <p>Port <input type="text" value="/1001"/></p> <p>Transport <input type="text" value="TLS"/></p> <p>Unified Communications services <input type="text" value="Yes"/></p> <p>TLS verify mode <input type="text" value="On"/></p> <p>Media encryption mode <input type="text" value="Force encrypted"/></p> <p>ICE support <input type="text" value="Off"/></p> <p>Poison mode <input type="text" value="Off"/></p>	Destination port Traversal Server is listening on Unified Communications must be enabled
<p><b>Authentication</b></p> <p>Authentication policy <input type="text" value="Do not check credentials"/></p>	Must be set to 'Do not check credentials' as expressway does not register any endpoints
<p><b>Client settings</b></p> <p>Retry interval <input type="text" value="120"/></p>	Must be FQDN Must be DNS resolvable Must match CN from certificate presented by Traversal Server (Expressway E)
<p><b>Location</b></p> <p>Peer 1 address <input type="text" value="expressway.vmgp.lab"/></p> <p><small>SIP: Reachable 10.48.35.171:7001</small></p>	

## Dominio servizi voce

L'utente accede sempre con **userid@domain4**, poiché non dovrebbe esserci alcuna differenza nell'esperienza dell'utente all'interno o all'esterno. Ciò significa che se **domain1** è diverso da **domain4**, è necessario configurare il dominio dei servizi voce nel client Jabber. Ciò è dovuto al fatto che la parte del dominio dell'accesso viene utilizzata per individuare i servizi di Collaboration Edge che utilizzano le ricerche dei record del servizio (SRV).

Il client esegue una query sui record SRV DNS (Domain Name System) per **\_collab-edge.\_tls.<domain>**. Ciò implica che quando il dominio dell'ID utente di accesso è diverso dal dominio dell'Expressway E, è necessario utilizzare la configurazione del dominio del servizio vocale. Jabber utilizza questa configurazione per individuare Collaboration Edge e UDS.

Per completare questa attività è possibile utilizzare diverse opzioni:

1. Aggiungere questo parametro quando si installa Jabber tramite MSI (Media Services Interface):

```
msiexec /i CiscoJabberSetup.msi VOICE_SERVICES_DOMAIN=domain1 CLEAR=1
```

2. Selezionare **%APPDATA% > Cisco > Unified Communications > Jabber > CSF > Config**, quindi creare il file **jabber-config-user.xml** nella directory:

```
<?xml version="1.0" encoding="utf-8"?>
<config version = "1.0">
<Policies> <VoiceServicesDomain>domain1</VoiceServicesDomain>
</Policies>
</config>
```

**Nota:** Questo metodo è solo sperimentale e non è ufficialmente supportato da Cisco.

3. Modificare il file **jabber-config.xml**. È quindi necessario che il client esegua prima l'accesso interno. Il [generatore di file di configurazione Jabber](#) può essere utilizzato per:

```
<Policies>
<VoiceServicesDomain>domain1</VoiceServicesDomain>
</Policies>
```

4. Inoltre, i client Jabber mobili possono essere configurati con il dominio dei servizi voce in anticipo, in modo che non debbano prima accedere internamente. Questa condizione viene spiegata nella Guida all'installazione e alla distribuzione nel capitolo [Service Discovery](#). È necessario creare un URL di configurazione su cui l'utente deve fare clic:

```
ciscojabber://provision?ServicesDomain=domain4&VoiceServicesDomain=domain1
```

**Nota:** È necessario utilizzare il dominio dei servizi voce perché è necessario verificare di eseguire la ricerca dei record di Collaboration Edge SRV per il dominio esterno (**dominio1**).

## Record DNS

In questa sezione vengono descritte le impostazioni di configurazione per i record DNS esterni e interni.

### Esterna

Tipo	Voce	Risolve in
record SRV	_collab-edge_tls.domain1	ExpresswayE.dominio1
Un record	ExpresswayE.dominio1	ExpresswayE indirizzo IP

È importante notare che:

- I record SRV restituiscono un nome di dominio completo (FQDN) e non un indirizzo IP.
- Il nome di dominio completo restituito dai record SRV deve corrispondere al nome di dominio completo (FQDN) effettivo di Expressway-E oppure la destinazione del record SRV è un nome di dominio completo (CNAME) e l'alias punta a un server nello stesso dominio di Expressway-E (ID bug Cisco in sospeso [CSCuo82526](#)).

Questa operazione è necessaria perché Expressway-E imposta un cookie sul client con il proprio dominio (**dominio1**) e, se questo non corrisponde al dominio restituito dall'FQDN, il client non lo accetta. l'ID bug Cisco [CSCuo83458](#) viene aperto come miglioramento in questo scenario.

### Interno

Tipo	Voce	Risolve in
record SRV	_cisco-uds._tcp.domain1	dominio.cucm3
Un record	dominio.cucm3	Indirizzo IP CUCM

Poiché il dominio dei servizi voce è impostato su **domain1**, Jabber incorpora **domain1** nell'URL trasformato per l'individuazione della configurazione di Collaboration Edge (**get edge\_config**). Una volta ricevuto, Expressway-C esegue una query sui record UDS SRV per **domain1** e restituisce i record nel messaggio **200 OK**.

Tipo	Voce	Risolve in
SRV	_cisco-uds._tcp.domain4	dominio.cucm3
Un record	dominio.cucm3	Indirizzo IP CUCM

Quando il client è in rete, il rilevamento dei record UDS SRV è necessario per **domain4**.

## Domini SIP su Expressway-C

È necessario aggiungere i seguenti domini SIP (Session Initiation Protocol) in Expressway-C e abilitarli per MRA:

Domains					You are here: <a href="#">Configuration</a> > Domains
Index	Domain name	Unified CM registrations	IM and Presence	Actions	
<input type="checkbox"/> 1	domain1	On	Off	<a href="#">View/Edit</a>	
<input type="checkbox"/> 2	domain4	Off	On	<a href="#">View/Edit</a>	

## Nome host/Indirizzo IP server CUCM

Unified CM server lookup

Unified CM publisher address:  ⓘ

Username:  ⓘ

Password:  ⓘ

TLS verify mode:  ⓘ

When TLS verify mode is on must match CN from Tomcat certificate

When TLS verify mode is off: ip address or hostnadr or fqdn from publisher

When TLS verify is On we need to make sure:

- CN must match address configured above
- Tomcat self signed certificate is added as Trust certificate or issuer of Tomcat Certificate is added as Trust certificate

Quando si configurano i server Cisco Unified Communications Manager (CUCM), si possono verificare due scenari:

- Se Expressway-C (**dominio2**) è configurato con lo stesso dominio del server CUCM (**dominio3**), è possibile configurare i server CUCM (**Sistema > Server**) con:

Indirizzo IP | nome host | FQDN

- Se Expressway-C (**dominio2**) è configurato con un dominio diverso dal server CUCM (**dominio3**), è necessario configurare i server CUCM con:

Indirizzo IP | FQDN

Questa operazione è necessaria perché quando Expressway-C individua i server CUCM e viene restituito il nome host, esegue una ricerca DNS per **nomehost.dominio2**, che non funziona se **dominio2** e **dominio3** sono diversi.

## Certificati

Oltre ai requisiti generali dei certificati, è necessario aggiungere alcuni elementi alla SAN (Subject Alternate Names) dei certificati:

- Expressway-C

È necessario aggiungere gli alias dei nodi di chat configurati nei server IM&P. Questa condizione è necessaria solo per le distribuzioni federative XMPP di Unified Communications che intendono utilizzare sia Transport Layer Security (TLS) che Group Chat. Questa opzione viene aggiunta automaticamente alla richiesta di firma del certificato (CSR), a condizione che siano già stati individuati i server IM&P.

È necessario aggiungere i nomi, in formato FQDN, di tutti i profili di sicurezza telefonica in CUCM configurati per TLS crittografati e utilizzati per i dispositivi che richiedono l'accesso remoto.

**Nota:** Il formato FQDN è necessario solo quando l'Autorità di certificazione (CA) non consente la sintassi del nome host nella SAN.

- Expressway-E

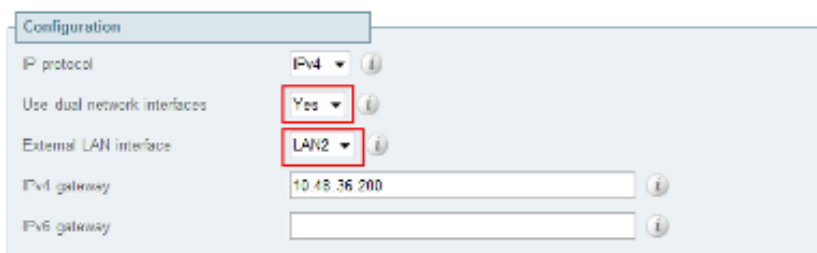
È necessario aggiungere il dominio utilizzato per l'individuazione del servizio (**dominio1**). Domini federativi XMPP. È necessario aggiungere gli alias dei nodi di chat configurati nei server IM&P. Questa condizione è necessaria solo per le distribuzioni federative XMPP di Unified Communications che intendono utilizzare sia TLS che Group Chat. Questi possono essere copiati dal CSR generato su Expressway-C.

## Doppia NIC

In questa sezione vengono descritte le impostazioni di configurazione quando si utilizzano schede di interfaccia di rete (NIC, Network Interface Card) doppie.

### Due interfacce

Quando si configura Expressway-E in modo da utilizzare interfacce di rete doppie, è importante verificare che entrambe le interfacce siano configurate e utilizzate.



The screenshot shows a configuration window titled "Configuration" with the following settings:

IP protocol	IPv4
Use dual network interfaces	Yes
External LAN interface	LAN2
IPv4 gateway	10.48.36.200
IPv6 gateway	

Use dual network interfaces set to Yes

External LAN interface used to connect to internet

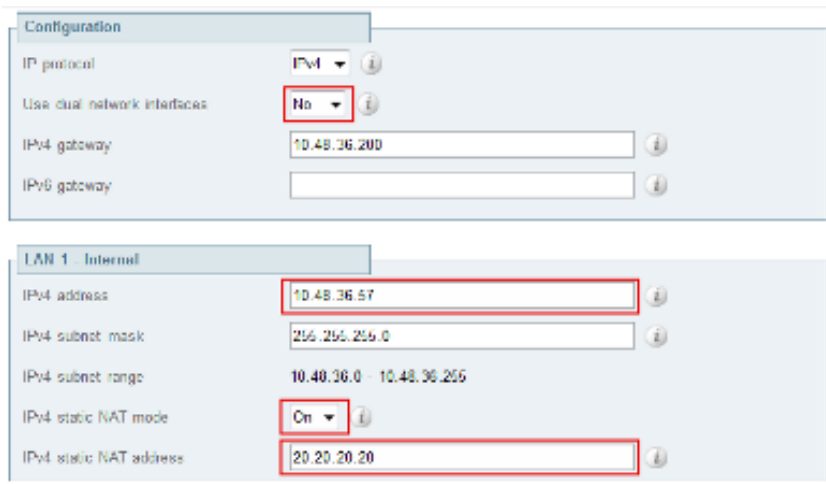
Quando il valore **Use dual network interfaces** è configurato su **Yes**, Expressway-E rimane in ascolto solo sull'interfaccia interna per la comunicazione XMPP con Expressway-C. È quindi necessario verificare che l'interfaccia sia configurata e funzioni correttamente.

### One Interface - Indirizzo IP pubblico

Quando si utilizza una sola interfaccia e si configura Expressway-E con un indirizzo IP pubblico, non è necessario tenere conto di considerazioni speciali.

## One Interface - Indirizzo IP privato

Quando si utilizza una sola interfaccia e si configura Expressway-E con un indirizzo IP privato, è necessario configurare anche l'indirizzo statico NAT (Network Address Translation):



The screenshot shows the configuration interface for Expressway-E. It is divided into two main sections: 'Configuration' and 'LAN 1 - Internal'. In the 'Configuration' section, the 'IP protocol' is set to 'IPv4', 'Use dual network interfaces' is set to 'No', the 'IPv4 gateway' is '10.48.36.200', and the 'IPv6 gateway' is empty. In the 'LAN 1 - Internal' section, the 'IPv4 address' is '10.48.36.57', the 'IPv4 subnet mask' is '255.255.255.0', the 'IPv4 subnet range' is '10.48.36.0 - 10.48.36.255', the 'IPv4 static NAT mode' is set to 'On', and the 'IPv4 static NAT address' is '20.20.20.20'. Red boxes highlight the 'No' dropdown, the 'IPv4 address' field, the 'On' dropdown, and the 'IPv4 static NAT address' field. To the right of the screenshot, there are three explanatory text blocks: 'Use dual network interfaces set to No', 'Private ip address of the Expressway-E', and 'Enabled static NAT Public ip address for which static NAT has been configured to the Expressway-E server'.

In tale situazione è importante garantire che:

- Expressway-C può essere utilizzato dal firewall per inviare traffico all'indirizzo IP pubblico. Questo processo è noto come *riflessione NAT*.
- La zona Traversal Client su Expressway-C è configurata con un indirizzo peer che corrisponde all'indirizzo NAT statico su Expressway-E, che in questo caso è **20.20.20.20**.

**Suggerimento:** Ulteriori informazioni sulle implementazioni di rete avanzate sono disponibili nell'**Appendice 4** della [Guida alla distribuzione di Cisco TelePresence Video Communication Server Basic Configuration \(Control with Expressway\)](#).

## Verifica

Attualmente non è disponibile una procedura di verifica per questa configurazione.

## Risoluzione dei problemi

Le informazioni contenute in questa sezione permettono di risolvere i problemi relativi alla configurazione.

In questa sezione vengono illustrati alcuni scenari specifici, ma è possibile utilizzare [Collaboration Solutions Analyzer](#), che fornisce una visualizzazione dettagliata di tutte le comunicazioni relative ai tentativi di accesso MRA e alle informazioni per la risoluzione dei problemi in base ai log di diagnostica.

## Zona trasversale



Quando l'indirizzo del peer è configurato come indirizzo IP o non corrisponde al nome comune (CN), nei registri viene visualizzato quanto segue:

```
Event="Outbound TLS Negotiation Error" Service="SIP" Src-ip="10.48.80.161"  
Src-port="25697" Dst-ip="10.48.36.171" Dst-port="7001" Detail="Peer's TLS  
certificate identity was unacceptable" Protocol="TLS" Common-name="10.48.36.171"
```

Se la password non è corretta, nei registri di Expressway-E verrà visualizzato quanto segue:

```
Module="network.ldap" Level="INFO": Detail="Authentication credential found in  
directory for identity: traversal"
```

```
Module="developer.nomodule" Level="WARN" CodeLocation="ppcmains/sip/sipproxy/  
SipProxyAuthentication.cpp(686)" Method="SipProxyAuthentication::  
checkDigestSAResponse" Thread="0x7f2485cb0700": calculated response does not  
match supplied response, calculatedResponse=769c8f488f71eebdf28b61ab1dc9f5e9,  
response=319a0bb365decf98c1bb7b3ce350f6ec
```

```
Event="Authentication Failed" Service="SIP" Src-ip="10.48.80.161"  
Src-port="25723" Detail="Incorrect authentication credential for user"  
Protocol="TLS" Method="OPTIONS" Level="1"
```

## Doppia NIC

Quando è abilitata la scheda di interfaccia di rete doppia ma la seconda interfaccia non è utilizzata o connessa, Expressway-C non è in grado di connettersi alla Expressway-E per la comunicazione XMPP sulla porta 7400 e i registri Expressway-C indicano quanto segue:

```
xwayc XCP_JABBERD[23843]: UTCTime="2014-03-25 17:19:45,843" ThreadID=  
"139747212576512" Module="Jabber" Level="INFO" CodeLocation="mio.c:1109"  
Detail="Connecting on fd 28 to host '10.48.36.171', port 7400"xwayc
```

```
XCP_JABBERD[23843]: UTCTime="2014-03-25 17:19:45,847" ThreadID="139747212576512"  
Module="Jabber" Level="ERROR" CodeLocation="mio.c:1121" Detail="Unable to  
connect to host '10.48.36.171', port 7400:(111) Connection refused"
```

```
xwayc XCP_JABBERD[23843]: UTCTime="2014-03-25 17:19:45,847" ThreadID=  
"139747406935808" Module="Jabber" Level="ERROR" CodeLocation=  
"base_connection.cpp:104" Detail="Failed to connect to component  
jabberd-port-1.expresswayc-vngtp-lab"
```

## DNS

Quando l'FQDN restituito dalla ricerca dei record SRV per Collaboration Edge non corrisponde all'FQDN configurato in Expressway-E, nei log di Jabber viene visualizzato questo errore:

```
WARNING [9134000] - [csf.edge][executeEdgeConfigRequest] XAuth Cookie expiration  
time is invalid or not available. Attempting to Failover.
```

```
DEBUG [9134000] - [csf.edge][executeEdgeConfigRequest]Failed to retrieve  
EdgeConfig with error:INTERNAL_ERROR
```

Nei log di diagnostica per Expressway-E, è possibile vedere per quale dominio il cookie è impostato nel messaggio HTTPS:

Set-Cookie: X-Auth=1e1111e1-dddb-49e9-ad0d-ab34526e2b00; Expires=Fri, 09 May 2014 20:21:31 GMT; **Domain=.vnntp.lab**; Path=/; Secure

## Domini SIP

Quando i domini SIP richiesti non vengono aggiunti in Expressway-C, Expressway-E non accetta messaggi per questo dominio e nei log di diagnostica viene visualizzato un messaggio **403** Non consentito inviato al client:

```
ExpresswayE traffic_server[15550]:  
Module="network.http.trafficserver" Level="DEBUG": Detail="Sending Response"  
Txn-id="2" Dst-ip="10.48.79.80" Dst-port="50314"  
HTTPMSG:  
|HTTP/1.1 403 Forbidden  
Date: Wed, 21 May 2014 14:31:18 GMT  
Connection: close  
Server: CE_E  
Content-Length: 0
```

```
ExpresswayE traffic_server[15550]: Event="Sending HTTP error response"  
Status="403" Reason="Forbidden" Dst-ip="10.48.79.80" Dst-port="50314"
```