

Checking the Status of Unified Communications Services

**Configuration checklist for DVO-R**

1. Set up Cisco Unified Communications Manager to support DVO-R.
2. Set up DVO-R for each device.
3. Set up user-controlled voicemail avoidance.
4. Add Remote Destination (optional).
5. Configure Cisco Jabber client settings.

See *Configuring Dial via Office-Reverse to Work with Mobile and Remote Access* at <http://www.cisco.com/c/en/us/support/unified-communications/expressway-series/products-configuration-examples-list.html> for more information.

## Checking the Status of Unified Communications Services

You can check the status of the Unified Communications services on both Expressway-C and Expressway-E.

1. Go to **Status > Unified Communications**.
2. Review the list and status of domains, zones and (Expressway-C only) Unified CM and IM&P servers.  
Any configuration errors will be listed along with links to the relevant configuration page from where you can address the issue.

## Mobile and Remote Access Port Reference

This section summarizes the ports that could potentially be used between your internal network (where the Expressway-C is located) and the DMZ (where the Expressway-E is located) and between the DMZ and the public internet.

**Outbound from Expressway-C (private) to Expressway-E (DMZ)**

Purpose	Protocol	Expressway-C (source)	Expressway-E (listening)
XMPP (IM and Presence)	TCP	Ephemeral port	7400
SSH (HTTP/S tunnels)	TCP	Ephemeral port	2222
Traversal zone SIP signaling	TLS	25000 to 29999	7001
Traversal zone SIP media (for small/medium systems on X8.1 or later)	UDP	36000 to 59999*	2776 (RTP), 2777 (RTCP) if <b>Use configured demultiplexing ports = Yes</b>  or 36000 (RTP), 36001 (RTCP) if <b>Use configured demultiplexing ports = No</b>
Traversal zone SIP media (for large systems)	UDP	36000 to 59999*	36000 to 36011 (6 pairs of RTP and RTCP ports for multiplexed media traversal)

Mobile and Remote Access Port Reference

**Outbound from Expressway-E (DMZ) to public internet**

Purpose	Protocol	Expressway-E (source)	Internet endpoint (listening)
SIP media	UDP	36002 to 59999 or 36012 to 59999	>= 1024
SIP signaling	TLS	25000 to 29999	>= 1024

**Inbound from public internet to Expressway-E (DMZ)**

Purpose	Protocol	Internet endpoint (source)	Expressway-E (listening)
XMPP (IM and Presence)	TCP	>= 1024	5222
HTTP proxy (UDS)	TCP	>= 1024	8443
Media	UDP	>= 1024	36002 to 59999 or 36012 to 59999*
SIP signaling	TLS	>= 1024	5061
HTTPS (only required for external administrative access, which is strongly discouraged)	TCP	>= 1024	443

**From Expressway-C to Internal Infrastructure and Endpoints**

Purpose	Protocol	Expressway-C (source)	Internal Device Port/Range
XMPP (IM and Presence)	TCP	Ephemeral port	7400 (IM and Presence)
HTTP proxy (UDS)	TCP	Ephemeral port	8443 (Unified CM)
HTTP proxy (SOAP)	TCP	Ephemeral port	8443 (IM and Presence Service)
HTTP/HTTPS (configuration file retrieval)	TCP	Ephemeral port	(Unified CM) HTTP 6970 <b>Or</b> HTTPS 6972 if you have Cisco Jabber 11.x or later with Unified CM 11.x or later
CUC (voicemail)	TCP	Ephemeral port	443 (Unity Connection)
Message Waiting Indicator (MWI) from Unity Connection	TCP	Ephemeral port	7080 (Unity Connection)
Media	UDP	36000 to 59999*	>= 1024 (Media recipient eg. endpoint)
SIP signaling	TCP	25000 to 29999	5060 (Unified CM)
Secure SIP signaling	TLS	25000 to 29999	5061 (Unified CM)

\* The default media traversal port range is 36000 to 59999, and is set on the Expressway-C at **Configuration > Local Zones > Traversal Subzone**. In Large Expressway systems the first 12 ports in the range - 36000 to 36011 by default - are always reserved for multiplexed traffic. The Expressway-E listens on these ports. You cannot configure a

## Enabling Support for Apple Push Notifications

distinct range of demultiplex listening ports on Large systems: they always use the first 6 pairs in the media port range. On Small/Medium systems you can explicitly specify which 2 ports listen for multiplexed RTP/RTCP traffic, on the Expressway-E (**Configuration > Traversal > Ports**). If you choose not to configure a particular pair of ports (**Use configured demultiplexing ports = No**), then the Expressway-E will listen on the first pair of ports in the media traversal port range (36000 and 36001 by default). **Note:** Changes to the **Use configured demultiplexing ports** setting need a system restart to take effect.

Note that:

- Ports 8191/8192 TCP and 8883/8884 TCP are used internally within the Expressway-C and the Expressway-E applications. Therefore these ports must not be allocated for any other purpose. The Expressway-E listens externally on port 8883; therefore we recommend that you create custom firewall rules on the external LAN interface to drop TCP traffic on that port.
- The Expressway-E listens on port 2222 for SSH tunnel traffic. The only legitimate sender of such traffic is the Expressway-C (cluster). Therefore we recommend that you create the following firewall rules for the SSH tunnels service:
  - one or more rules to allow all of the Expressway-C peer addresses (via the internal LAN interface, if appropriate)
  - followed by a lower priority (higher number) rule that drops all traffic for the SSH tunnels service (on the internal LAN interface if appropriate, and if so, another rule to drop all traffic on the external interface)

## Enabling Support for Apple Push Notifications

This feature applies if you have Cisco Jabber users with iOS devices (Cisco Jabber for iPhone and iPad) who sign in remotely. Expressway deployments that are configured for MRA can support Apple's cloud-based Push Notification service. From X8.9.1, we supported Push Notifications for IM and Presence Service instant messages. From X8.10, we support them for voice and video calls too. Push Notifications are only used for Jabber for iPhone and iPad clients. Android, Windows, and Mac users are unaffected.

**Note:** If Unified CM detects a remote or mobile Jabber for iPhone and iPad connection, it always sends a Push Notification as well as a SIP Invite.

### Prerequisites and recommendations

No specific configuration is needed on the Expressway for Push Notifications, assuming Expressway-E is already providing Mobile and Remote Access (MRA) for Jabber iOS devices. However, these prerequisites and recommendations apply:

- Push Notifications in the Expressway require a network connection between Expressway and the Cisco WebEx cloud, and between Cisco Jabber and the Push Notification servers in the Apple cloud. **They cannot work in a private network, with no internet connection.**
- MRA must be fully configured (domain, zone, server settings).
- Depending on your Unified CM configuration, the Unified CM may need a forward proxy to send Push Notifications to the Cisco Collaboration Cloud.
- We recommend using self-describing token authorization.
- Expressway-E **restart required for Push Notifications with instant messages**. After you enable Push Notifications on the IM and Presence Service you need to restart the Expressway-E. Until the restart, Expressway-E can't recognize the push capability on IM and Presence Service, and does not send PUSH messages to the Jabber clients.
- You need the following Push Notification-enabled releases (or higher) on Cisco Unified Communications Manager, IM and Presence Service, and the Jabber devices: