

Office Communications Server 2007 Standard Automatic Client Sign-In

This following document highlights the important aspects of the aforementioned document as it pertains to automatic client sign-in.

ABSTRACT

Microsoft OCS clients (a) are capable of automatic sign-in or more accurately, automatic client configuration. In short, the end user need only provide their email address and domain password to the OCS client to log into the appropriate OCS server.

(a) OCS clients capable of automatic sign-in include Microsoft Office Communicator, Microsoft Messenger for the Mac, Enterprise Messenger on the BlackBerry, and Microsoft Communicator Mobile for Windows Mobile.

Client sign-in process

(1) The OCS client queries for specific DNS SRV records based on the domain name of the user's email address. These queries are hard coded into the OCS client as follows and occur in this order (tld.com /top level domain/ would be the root domain name of the enterprise, ex. mycompany.com):

_sipinternaltls._tcp.tld.com -> 5061 ocs_server.tld.com / for internal TLS connections
_sipinternal._tcp.tld.com -> 5060 ocs_server.tld.com / for internal unencrypted connections
_sip._tls.tld.com -> 5061 ocs_server.tld.com / for external TLS connections
_sip._tcp.tld.com -> 5060 ocs_server.tld.com / for external unencrypted connections

If no valid SRV records are returned, the OCS client will query a record for the following to attempt the connection

sipinternal.tld.com
sip.tld.com
sipexternal.tld.com

(2) The OCS client will attempt a connection to the OCS server using the first valid response from the queries made above.

(3) If the first response is a TLS connection with a trusted SSL server certificate, the connection establishes and login succeeds assuming credentials are validated. If the server provides an invalid certificate, the connection is terminated and no further attempts are made to establish a connection. If no valid SRV or A records are found, the client will return a connection error.

To summarize, the three important aspects of a successful OCS Automatic Client Sign-In deployment are these:

- (A) Correctly configured DNS SRV and A records
- (B) Correctly configured firewall that allows port 5061 for TLS or 5060 for unencrypted connections
- (C) Valid SSL Certificate for the OCS Server

DETAILS

(A) DNS SRV Records

At least one of the SRV or A records previously mentioned need to exist for automatic client sign-in to function. If TLS encryption is necessary then the unencrypted entries should be left out and port 5060 should stay closed on the firewall. For instance, if we wanted to force TLS encrypted sessions to both internal and external clients, the DNS SRV entries would look like the following (for the domain mycompany.com and an OCS Server with the hostname of ocs_server):

```
_sipinternaltls._tcp.tld.com.mycompany.com.  IN  SRV  0 0 5061 ocs_server.mycompany.com.  
_sip._tls.mycompany.com.                    IN  SRV  0 0 5061 ocs_server.mycompany.com.  
sip.mycompany.com                          IN  A      x.x.x.x
```

Note: sip.mycompany.com should point to the IP address of the OCS Server; a CNAME would also work. This entry isn't a hard requirement; it is used as a fallback if no SRV records are returned.

(B) Firewall Settings

There are a large number of ports that OCS requires depending on the feature-set your enterprise requires. Since this document pertains to just automatic client sign-in we are only concerned about two. For unencrypted connections, TCP port 5060 needs to be opened on the external interface. For encrypted connections, TCP port 5061 needs to be opened on the external interface. For a complete list of required ports for OCS, see page 71 of the OCS_Planning_Guide.doc as mentioned previously.

(C) SSL Certificate

A third-party trusted SSL certificate needs to be acquired for TLS encrypted OCS connections. This is unnecessary if sole use of unencrypted connections are to be used. The kind of SSL certificate that is needed will depend on whether or not the enterprise uses

- a. Split-Horizon (a.k.a. split-brain) DNS or maintains separate: In the split-horizon DNS topology, a single domain name is used both internally and externally. Requests to the DNS server from the internal network returns internal IPs to clients located on the internal network. Requests to the

DNS server from an external network returns external IPs to clients not located on the internal network.

- b. Internal and external DNS domains: In the separate internal and external DNS domain topology, different domain extensions are commonly used to separate the internal and external domains. For example, the internal name for an OCS server in this topology could be `ocs_server.mycompany.local` while the external name would be `ocs_server.mycompany.com`.

In either scenario, you'll need to ensure you purchase an SSL certificate that supports multiple Subject Alternative Names (SAN). At a minimum, you'll need to create an SSL certificate with the following attributes (assuming the name of the OCS server is `ocs_server` and the domain is `mycompany.com`):

- a. Split-horizon DNS SSL Certificate:
 - Subject: `ocs_server.mycompany.com`
 - Subject Alternative Names: `sip.mycompany.com`

- b. Separate internal and external DNS domains SSL Certificate
 - Subject: `ocs_server.mycompany.com`
 - Subject Alternative Names: `sip.mycompany.com`
 - `ocs_server.mycompany.local`
 - `sip.mycompany.local`

As you can see the split-horizon topology demands fewer SAN's. Self-signed SSL certificates can also be used provided the OCS clients have the appropriate SSL root certificate installed and trusted.