Surround SCM Proxy Server Best Practices

Proxy servers, which are installed on a local network, cache files requested by Surround SCM clients from locations that are remote from the master Surround SCM Server. Subsequent requests for the files are handled by the proxy server instead of the Surround SCM Server. This decreases network usage and response time.

Surround SCM clients only use the proxy server to get files. Adds, check ins, and check outs are still performed on the master server. The proxy server acts as another client attached to the master server. The master server only sends data to the proxy server when the proxy server requests it. The data saved in the proxy server cache is a copy of data from the master server and does not need to be backed up.

Controlling what is cached

When a remote client performs a get, the master server provides the client with a key for the requested file version. The client uses the key to connect to the proxy server and request the file. If a copy of the file that corresponds to the key already exists in the proxy server cache, the proxy server sends the file to the client. If the file does not exist, the proxy server retrieves the file from the master server, saves it in the cache, and then sends it to the client.

Keep in mind that there is some additional overhead when a client gets a file from the proxy server because additional network transactions are required. However, in most cases, it takes far less time to perform the local network transactions than it takes to retrieve the file from the remote master server. For smaller files, it is often faster to get the file from the master server.

The Minimum file size for cache option controls the size of files cached by the proxy server. If a user gets a file that is smaller than the minimum cache file size, it is retrieved from the master server.

The minimum file size setting to use depends on the bandwidth and the type of connection between the clients, the proxy server, and the master server. The default value is 500 MB.

Do not set the minimum file size to zero because it will cause the proxy server to communicate with both servers for every get. The additional network transactions required can slow performance.

You may want to consider using a proxy server to improve retrieval of binary files. When retrieving large binary files from Surround SCM, performance may be slow due to the large amount of data that needs to be retrieved from the database. You can use a local proxy server to improve local performance when getting large binaries by installing the proxy server on the same computer as the master server. Set the minimum cache file size to a large number (e.g., 100 MB).
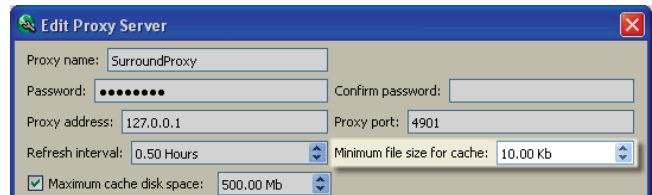

Figure 1: Minimum file size for cache setting

Managing proxy server disk space

The proxy server caches files until it runs out of disk space. While you can manually delete cached files or create a batch script to flush the cache, you can automatically manage the cache using the disk space and age limit options.

The Maximum cache disk space option controls the size of the cache folder. When the cache reaches the maximum size, the server overwrites older files in the cache. Do not set the cache disk space to be larger than the hard drive where the cache is stored.

The Age limit option specifies the number of days before the proxy server deletes cached copies of files.

When both options are set, the proxy server deletes files when the cache exceeds the allowable disk space even if the files have not exceeded the age limit. It also deletes files that exceed the age limit even if the cache is below the maximum limit.
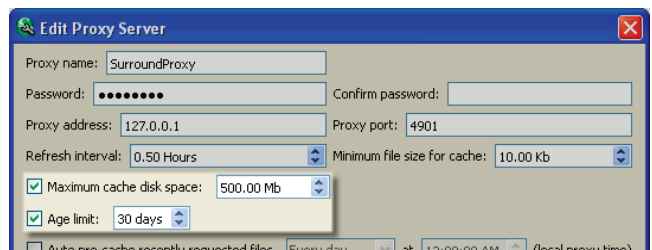

Figure 2: Maximum cache disk space and age limit options

Configuring encryption

By default, Surround SCM clients and the proxy server communicate with the master server on port 4900. Clients connect to the proxy server on port 4901. For the master server, you do not need to open the firewall to port 4901. The proxy server and master server do not communicate on that port. You can use a local DNS for the proxy server to ensure that no one outside your organization can access it.
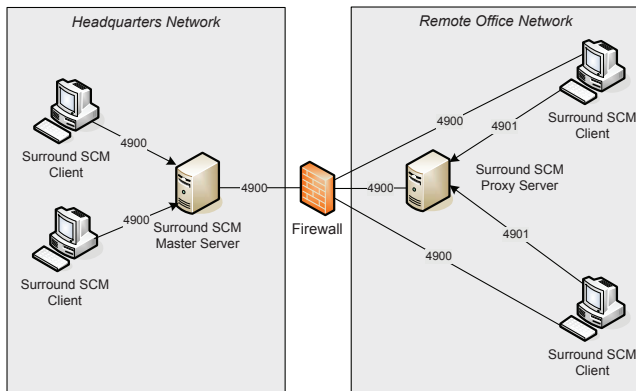

Figure 3: Proxy server configuration example

Using a VPN connection between the two servers or between the clients and the servers can eliminate the need for encryption. If you do not have a secure VPN connection between the master server and the proxy server or between the clients and the proxy server, you should set the encryption options. Encryption provides a higher level of security, but may slow performance due to the time spent to encrypt and decrypt messages.

The Encrypt transactions between proxy server and master server option encrypts messages sent between servers. Messages and file transfers are encrypted with a 512-bit key. The Encrypt transactions between proxy server and clients option encrypts messages sent between the proxy server and Surround SCM clients.
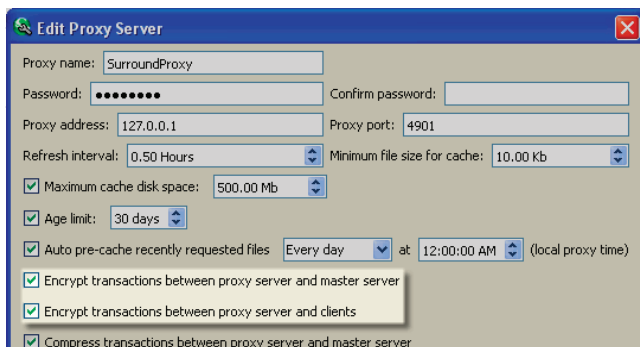

Figure 4: Encryption options

Pre-caching files

The first user to perform a get on a file takes the performance hit. This is not an issue when users get a few files, but users may experience a long wait if they are getting an entire branch. You can avoid this by pre-caching recently requested files. This ensures that frequently accessed files are already in the cache.

The Auto pre-cache recently requested files option evaluates the last 1,000 files. If you need to pre-cache more than 1,000 files, we recommend using a batch file to pre-cache the files on a regular basis.
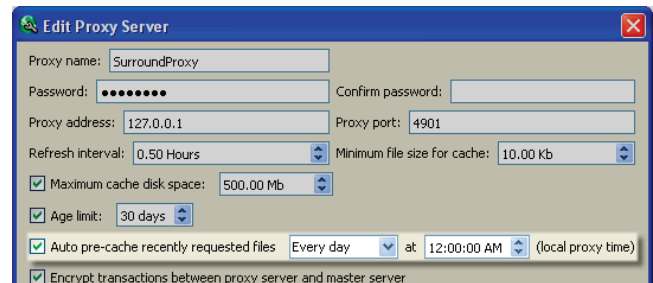

Figure 5: Auto pre-caching options

Optimizing performance

Because the proxy server is in a remote location, the transfer speed between it and the master server will not be the same as it is for a client accessing a local master server. The Compress transaction between proxy server and master server option can improve the transfer speed between servers over a slower connection.

You can also improve performance by storing the proxy cache on the fastest network storage device, preferably an internal hard drive. Using a shared network resource or an array may slow performance.
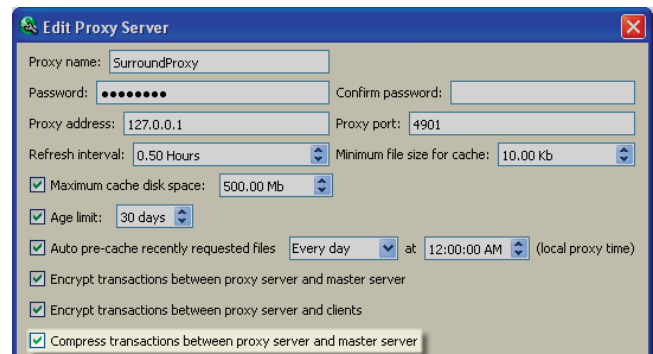

Figure 6: Compression options

Seapine Software™