Configuring the SBC Edge for Active Directory

This page explains how to configure the Ribbon SBC Edge to use Active Directory services.

⚠ Active Directory is always enabled by default, no licensing action is required to turn it on.

This process comprises three parts:

- Active Directory Configuration
- Cache Settings
- User Authentication Settings

The Active Directory configuration part is where you turn on Active Directory (AD), set the way the Ribbon SBC Edge will communicate with the AD server.

ⓘ The maximum amount of characters for the Active Directory Configuration attributes is 512.

The Cache Setting part is where you set up AD attribute caching.

The User Authentication Settings section is where you determine which domain controllers to use.

ⓘ For additional information about Active Directory, see Call Routing Based on Active Directory User Attributes and Basic AD-based Call Routing for Dummies.

Before You Begin

Before you begin, there some things you need to decide:

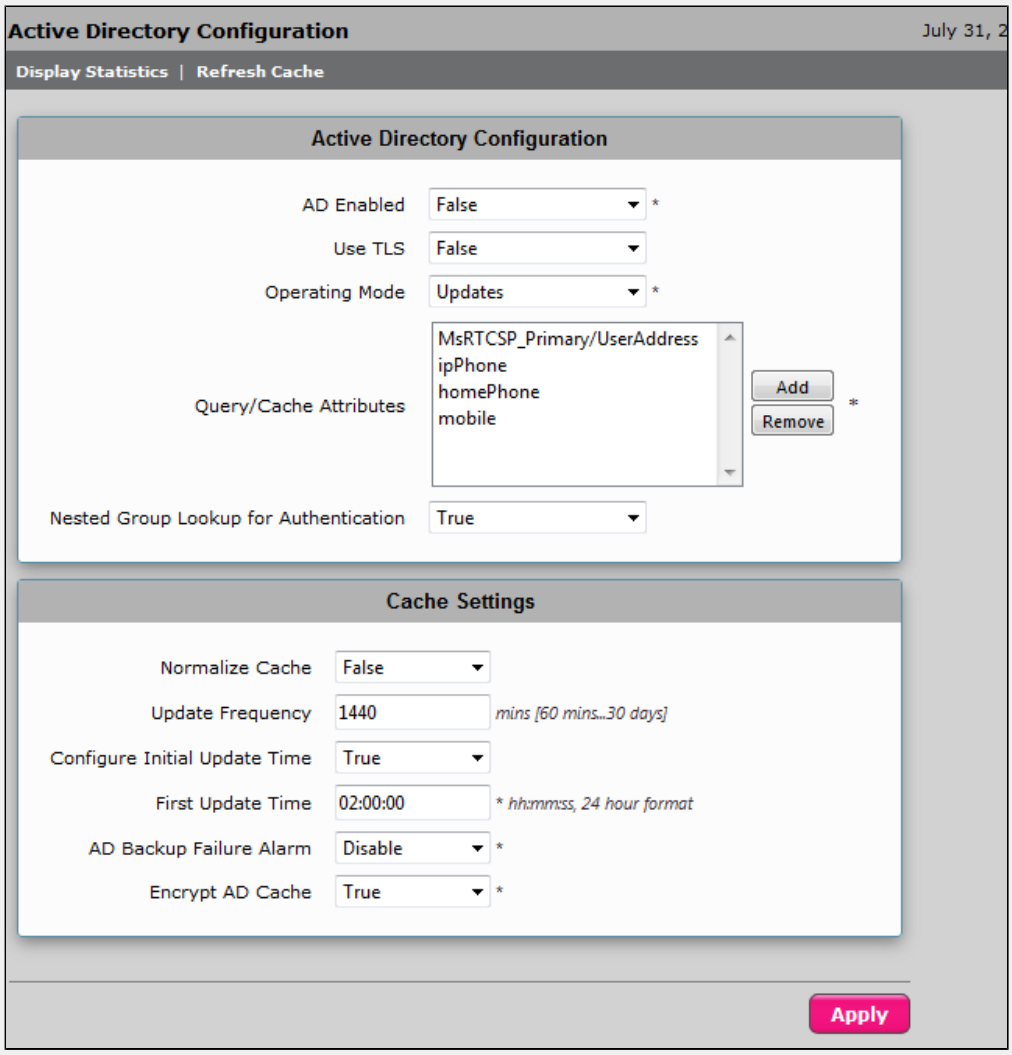
- Whether or not you are going to use TLS.
- What operating mode you intend to use.
    - Updates - a local cache is built and used to look up AD searchable fields. User authentication is enabled in this mode.
    - Online - Communication with Active Directory is done with queries and no information is cached.
    - Auth-only - This mode allows user authentication using Active Directory, and no queries are allowed.
    - Cache Lookup Only - When selected the SBC examines only the local AD Cache for the requested attribute, if none is found the call fails.

You must have already defined and added at least one domain controller to the Domain Controllers Table.

Configuring Active Directory Services on the SBC Edge

1. In the WebUI, click the **Settings** tab.
2. In the left navigation pane, go to **Auth and Directory Services > Active Directory > Configuration**.

Figure 1: Active Directory Configuration



Active Directory Configuration - Field Definitions

The fields in the Active Directory Configuration panel determine the manner in which Ribbon SBC Edge communicates with the Active Directory server.

AD Enabled

Specifies the administrative state of the Active Directory resource.

Use TLS

Specifies whether or not Transport Layer Security (TLS) is used while communicating with Active Directory.

- TLS = FALSE: MD5 Digest is used to secure the AD password over the wire.

> Since **DCs do not support referral chasing or nested group lookups with MD5 Digest**, you can't log in to SBC Edgeusing AD credentials if those credentials require referral chasing or nested group lookup by the DC. Instead, you can individually configure each DC you wish to query when someone attempts to log into the SBC Edge.

- TLS = TRUE: TLS will be used to secure all communcation for requests to the DC.

> Referral chasing and nested group lookups are supported with TLS enabled. Again, this applies only to authenticating users attempting to log into the Ribbon SBC Edge.

> AD lookups for **call routing** are executed the same regardless of the AD TLS configuration. **DCs do not support referral chasing for call route lookups**, therefore you must individually configure each DC that you wish to search for AD call routing queries.

Operating Mode

Specifies the method used by the Ribbon SBC Edge to communicate with Active Directory in order to achieve a balance between performance and accuracy.

- **Online:** All AD queries are sent directly to the DC - no information is cached. User authentication using Active Directory is also enabled in this mode. Online mode can result in a heavy DC load, thus using Online mode is not recommended.
- **Updates:** In this mode, a local cache is built and used to lookup Active Directory searchable fields. If the SBC's cache is filled to capacity, first the cache, then the DC will be queried in attempts to find a match. User authentication using Active Directory is also enabled in this mode; however, sensitive information (including passwords) is not cached.
- **Auth-Only:** Allows user authentication using Active Directory, but no Active Directory queries are allowed.
- **Cache Lookup Only:** When selected, the SBC examines **only** the local AD Cache for the requested attribute. Even if the cache is filled to capacity, the DC will not be queried. The call fails if no match is found in the local cache.

> **SBC 1000 Note:**
> Ribbon recommends the use of an external USB or ASM module for AD Cache backup on the SBC 1000 when either the **Upd ates** or **Cache Only** mode is the selected operating mode.

> An SNMP alarm will be generated if the local AD cache reaches capacity.

> If your cache reaches capacity when in Update Mode, the SBC will automatically query the DC for any entries that are not cached. Queries to the DC are never normalized. Routing may intermittently fail if your transformations rely on normalized cache entries.

> Be aware that Cache Normalization is not performed on queries to the DC, even in Update Mode with *Normalize Cache* set to *True*. Therefore, transformations that rely on normalization (e.g. msRTCSIP-Line transformations that do not include tel:) will fail for queries that resort to a DC lookup. If you're cache reaches capacity:
>
> - Reduce the number of cached attributes so that the cache is no longer at capacity
> - Set *Normalize Cache* to *False* and modify any transformation that relies on the cache being normalized. (suggested)
> - Add transformations to route both normalized and non-normalized AD call route queries. (avoid)

Query/Cache Attributes

Specifies which attributes are cached from Active Directory. The attribute names specified must be consistent with attribute names in Active Directory.

Nested Group Lookup for Authentication

Specifies whether or not nested group lookups are performed to authorize users. Applies only to authentication domain controllers.

Cache Settings - Field Definitions

The fields in the Cache Settings panel determine how Active Directory attributes are cached locally and the frequency at which the local cache is updated. The SBC Edge maintains a local cache of Active Directory user attributes. AD caching enhances system performance and survivability.

- **Performance:** Performance is enhanced by eliminating the need to communicate with and query the Active Directory server for each and every call. This improves the performance of the AD server, and has the added benefit of increasing call speeds and relieving load on the network.
- **Survivability:** In the event of a loss of communication with the Active Directory, whether through a loss of network connectivity or an AD server error, the SBC Edge is still able to perform authentication and authorization tasks based on the Local AD Cache.

Normalize Cache

Specifies whether or not to strip special characters such as dashes "-", parenthesis "(", ")", spaces " ", "tel:" and "sip:" from the values while building a local active directory cache. However, normalization does not apply to name and email fields.

Update Frequency

Specifies the interval, in minutes, between local Active Directory cache updates.

The Local AD Cache can be updated manually at any time by clicking the **Refresh Cache** text at the top of the Active Directory Configuration page.

Manually refreshing the cache is a one-time operation only. It will **not** affect the timing in which automatic cache refreshes occur.

Configure Initial Update Time

Specifies when the AD Cache is updated upon initial SBC power up or after an AD Configuration has been edited and applied. If set to **True**, the system waits until the time specified in the **First Update Time** field before updating the AD Cache. If set to **False** the AD Cache is updated immediately upon start up or when a new/edited configuration is applied.

First Update Time

Specifies the time (system time) at which the first AD Cache update occurs after initial SBC power up or after an AD Configuration has been edited and applied. This field is visible only when the **Configure Initial Update Time** field is set to **True**.

The last saved AD Cache is used until the first update specified by this field occurs.

On the SBC 2000 or the SBC 1000 (if it has an external external USB or ASM module), it is recommended to do the following

1. Set **Update Frequency** to 1440 minutes (24 hours)
2. Set **Configure Initial Update Time** to True
3. Configure **First Update Time** in a 24 hour format

The preceding procedure ensures that the cache refresh will always occur at a desired time instead of a random time. Only increase the cache Update Frequency to occur more often if there are frequent changes to the Windows Domain Controller; otherwise, once every 24 hours should be sufficient.

AD Backup Failure Alarm

When **Enabled**, the SBC will raise an alarm and send an SNMP Trap if the AD Cache backup fails. This parameter controls the alarm and trap generation only. It does not control the AD Cache backup function.

Encrypt AD Cache

NOTE: The Encrypt AD Cache is available on the SBC 1000 and SBC 2000 only.

The Encrypt AD Cache option allows the SBC Edge (SBC 1000, SBC 2000) to encrypt the AD cache when stored on any media (internal eUSB, external USB, or ASM). The AD cache contents can then only be viewed when it is decrypted with the correct password. This encryption secures the contents against unauthorized viewing.

Valid options: **True** (encrypts the AD cache) or **False** (does not encrypt the AD cache). Default entry: **False.**

Managing Active Directory Caching and Statistics

Configuring the SBC Edge for Active Directory User Domain Access

Configure SBC Edge for a Double-Equal AD Lookup