Some Help With

Mastering ACLs and Namespaces for Enhanced Security Management in Professional Environments

TABLE OF CONTENT

- Setting Up ACLs and Custom Namespaces
- Identifiers and Aliases
- The Role of Access Lists
- Managing Access with Wildcards
- Conclusion

Welcome to our discussion on Access Control Lists (ACLs) and the concept of namespaces. These two elements are vital for managing access and security in any professional environment.

Setting Up ACLs and Custom Namespaces

You can configure ACLs directly from the AnyDesk client under the access security settings, or through the admin portal at **my.anydesk.com** when creating custom clients.

Identifiers and Aliases

Let’s dive in! Every device connected to the AnyDesk network has a unique identifier. Initially, this identifier is a numerical value. Users with a paid license have the advantage of replacing this identifier with an alias, which is much easier to remember. This modification can be made by right-clicking the identifier to select the alias, or by accessing the client details in **my.anydesk** and editing the respective client.

An alias consists of two main parts: a unique identifier and a customizable namespace. Companies can acquire a private, unique namespace which enables them to align their devices with their corporate identity, simplifying the management of a large number of devices.

 © 2026 www.some

The Role of Access Lists

Now, let’s turn our attention to access lists. Think of them as a guest list for a restaurant or an event; if you’re on the list, you’re in. If not, entry is denied. Technicians aiming to connect to a device with access lists enabled must be on the list for the connection to be granted. If they aren’t, the connection will be immediately rejected.

Large teams with numerous users can find it challenging to manage these access lists. For instance, imagine having 100 service technicians. With regular changes in staff, either through new hires or departures, managing these extensive lists can become quite a task. This is where a custom namespace comes in handy; by incorporating any identifier within that namespace into the list, you automate the process.

Managing Access with Wildcards

Access lists can include individual identifiers, numerical IDs, and wildcards. The use of wildcards is crucial for dynamic and streamlined security management within large groups. Here’s how it works: by creating wildcards, you can form groups. For example, let’s say you have three groups of technicians. Those who need access to database servers can have “Senior Tech” within their identifiers. By simply adding `*Senior Tech` to your ACL, all eligible technicians gain access, while others are restricted.

Should a technician like Lou leave the organization, he will no longer be able to connect to devices he once had access to—even if he knows the ID and password. This highlights the importance of implementing Access Control Lists and acquiring a custom namespace to boost the security of your installation and facilitate the management of security in large support groups.

Conclusion

In conclusion, understanding and utilizing ACLs and namespaces are essential for improving security protocols in any environment with multiple access points. By adopting these measures, you can ensure a more secure and efficiently managed infrastructure.

 © 2026 www.some