Some Help With

Security tips and offboarding

TABLE OF CONTENT

Security features in the AnyDesk client

Access Control List (ACL)

On-Premises solution

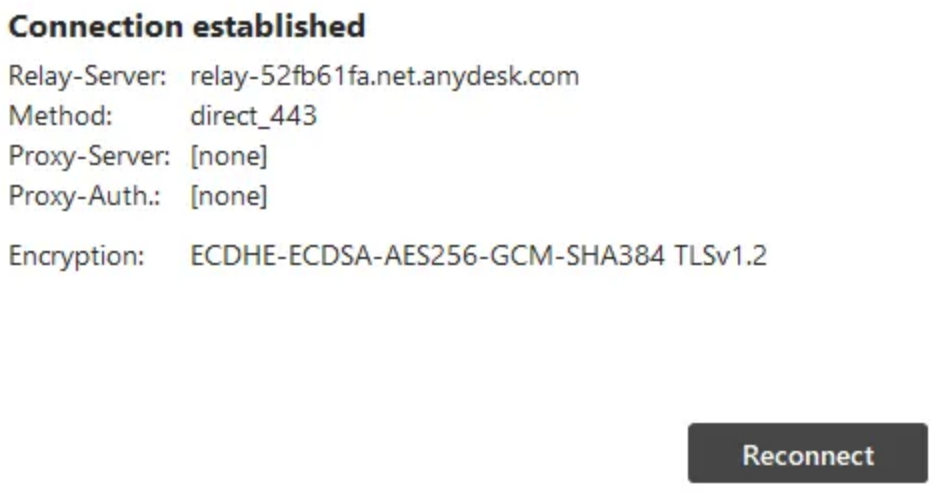
Offboarding former employees

All AnyDesk sessions are secured using **TLS 1.2** with **AEAD encryption**.

You can view the connection type, enforced encryption mode, client verification status, and fingerprint by clicking

Connection Info

in the toolbar.



VirtualBoxVM_Hvklu135vO

Security features in the AnyDesk client

AnyDesk provides several security features to help you protect your environment:

- **Custom client settings** - configure security policies in your custom client. For details, see Custom AnyDesk client.
- **Exclusive unattended access** - access the remote device only by using only the unattended password.
- **Salted password hashing** - passwords are securely stored using salted hash tokens.
- **Two-factor authentication** - protect unattended access by enabling two-factor authentication.

Access Control List (ACL)

You can restrict incoming sessions using the Access Control List to allow only authorized IDs or aliases.

On-Premises solution

For high-security environments, AnyDesk offers an On-Premises deployment option. This version operates independently of the internet, giving you full control over your data.

Offboarding former employees

If an employee using AnyDesk leaves your organization, take the following steps to protect your environment:

1. **Remove their client**
   If you know the AnyDesk ID or alias of the employee, in my.anydesk II, go to the *Clients* tab and remove their client. This revokes their access to your address book.
2. **Reset your license key**
   If they have access to the current license key, you can reset it in my.anydesk II > *License* > *About* > *Reset*. Removing the license key from their client will downgrade it to a free license.
3. **Restrict access to public custom clients**
   If your public custom client URLs are compromised, either make them private or recreate them to generate new links. Already installed copies won't be affected, you must also manually remove them from your license.

4. **Change unattended access passwords**
   Update all unattended access passwords that may have been shared or saved.
5. **Use the Access Control List (ACL)**
   The most effective way to prevent access is by configuring the ACL on each client to block the former employee's ID or Alias. Even if they know your passwords, they won't be able to connect if they're not whitelisted.
6. **Leverage custom namespaces**
   For easier management, consider purchasing a custom namespace. ACLs support wildcard values, so you can restrict access to sessions matching `*@yourcompanyname`. If you remove the license key from a former employee's client, the alias with your namespace is removed automatically, blocking them from connecting.