Okta Advanced Server Access (ASA) - End User Guide

# 1. Introduction

Okta Advanced Server Access (ASA) is a cloud-based solution that provides secure, passwordless, and role-based access to both on-premises and cloud servers. Instead of managing static SSH keys or RDP credentials, ASA uses short-lived certificates that are generated on-demand. This ensures that server access is more secure, easier to manage, and aligned with modern Zero Trust security principles.

Why this matters for you:

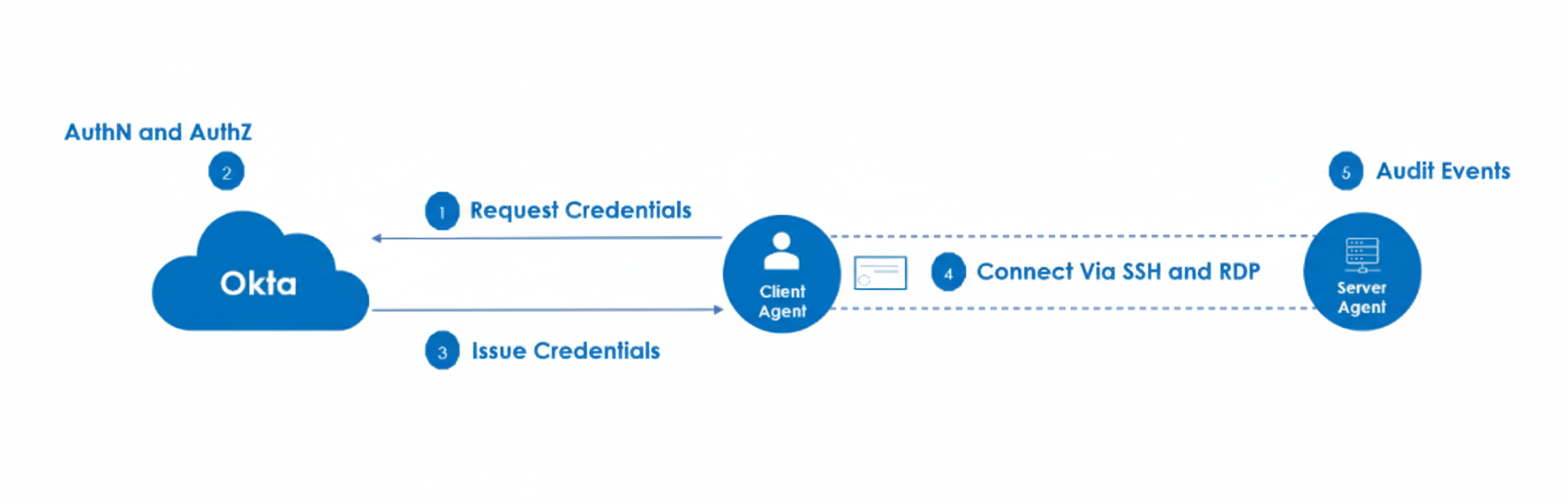
- Passwordless login → No need to remember SSH keys or RDP passwords.

- One-click access → Connect to your servers directly from your Okta dashboard.

- Secure by design → Every login is verified with Okta MFA and policy.

- Audit-ready → All access events are logged for compliance.

### ****2. Working Flow (Simple for End Users)****

Here’s how it works when you log in:

1. **Request Access** – You (client) try to connect to a server using the ASA Client Agent.
2. **Authenticate with Okta** – Okta checks your identity (username, password, MFA, etc.).
3. **Get Credentials** – Okta issues a short-lived certificate just for this session.
4. **Connect to Server** – Using that certificate, you connect directly to the server (SSH for Linux or RDP for Windows).
5. **Audit Logged** – The Server Agent records the event (who logged in, when, from where).

👉 The key idea: **No passwords or static keys. Every login is verified with Okta and gets a temporary certificate, which expires quickly.**

# 3. Installing the Okta ASA Client (Windows)

1. Go to the download link provided by IT: [Link: Okta ASA Client for Windows]

2. Download the MSI installer (latest stable version).

3. Run the installer by double-clicking the .msi file.

4. Follow the installation wizard:

- Click Next → Accept license → Install → Finish.

5. Once installed, the ScaleFT Client Tool (Okta ASA client) is available on your machine.

3. Once installed, open Command Prompt and run:  
  
 sft --version  
  
If you see a version number, installation was successful.

## 4. Enrolling Your Windows Client

After installing the client, you need to **enroll** your machine with Okta ASA.

1. Open **Command Prompt (cmd)** as administrator.
2. Run the following command:
3. sft enroll
4. A browser window will open automatically:
   * Enter your **Team Name** (provided by IT, e.g., okta-demo).
   * You’ll be redirected to the **Okta login page**.

[Screenshot: Okta login prompt]

1. Enter your **Okta credentials** (username + password + MFA).
2. Approve the consent window.
3. Once complete, your client is now enrolled.

✅ You can verify enrollment in two ways:

* Check via command:
* sft list-servers
* Or log into **ASA Dashboard** → **Clients** → See your device listed.

## 5. Accessing Servers

Now that your client is enrolled, you can connect to assigned servers directly.

### Option A: From Okta Dashboard (Web Portal)

### 5****.1 Access Linux Servers (SSH)****

1. Open **Okta Dashboard** → Click **Advanced Server Access App**.
2. Select the **Linux server** from the list → Click **Connect**.
3. A consent window appears → Click **Approve**.
4. A PowerShell window opens and you are logged into the Linux server securely via SSH.

[Screenshot: Linux server SSH session]

### ****5.2 Access Windows Servers (RDP)****

1. Go to **Okta Dashboard** → Open **Advanced Server Access App**.
2. Select the **Windows server** from the list → Click **Connect**.
3. When prompted, click **Open ScaleFT**.
4. Accept the certificate → An RDP window launches.
5. You are now securely connected to the Windows server.

[Screenshot: RDP session to Windows server]

### ****Option B: From Command Line****

* **List available servers**:
* sft list servers
* **Connect to Linux server (SSH)**:
* sft ssh <server-name>
* **Connect to Windows server (RDP)**:

sft rdp <server-name> (Courier New)

### ****6. Quick Commands Reference****

| **Command** | **Purpose** |
| --- | --- |
| sft --version | Checks ASA client version |
| sft enroll | Enrolls your client with Okta ASA |
| sft list servers | Shows servers you can access |
| sft ssh <server> | Connects to Linux server via SSH |
| sft rdp <server> | Connects to Windows server via RDP |
| sft unenroll | Unenrolls your client from ASA |
| sft login | Logs in and obtains fresh credentials |
| sft logout | Logs out your client and clears credentials |
| sft whoami | Displays the currently authenticated user and team |
| sft help | Shows a list of commands or help for a specific command |

👉 If you want to know more about ASA commands, please refer to the official documentation:  
Okta ASA CLI Reference

# 6. Troubleshooting

|  |  |
| --- | --- |
| **Issue** | **What it means & How to fix** |
| **sft enroll not working** | Your ASA client may not be installed properly. Try reinstalling the ASA client. Also, verify you entered the correct **Team Name** during enrollment. Ensure your system has internet connectivity and that the ASA client service (sftd) is running. |
| **Cannot see any servers** | You may not be assigned to the correct group/project. Contact your IT admin to ensure your account has the right server assignments. |
| **Session expired** | ASA uses short-lived certificates for security. If your session expires, run **sft enroll** again or reconnect from the ASA dashboard. |
| **Consent window not appearing** | Check your browser settings and disable pop-up blockers for the Okta ASA page. |
| **RDP connection fails** | Ensure **Remote Desktop** is enabled on your Windows machine and on the target server. Verify your firewall and internet connection. |
| **MFA issues** | Ensure your Okta MFA device (phone, email, or authenticator app) is working correctly and follow the prompts during login. |
| **System clock issue** | Certificates are time-sensitive. Ensure your system clock is accurate. |

# 7. Support

For any issues or questions regarding Okta ASA, please contact IAM Engineering team or raise a SNow ticket.