AnnTac

Uplink Server

Administrator guide

Installation, three deployment scenarios, accounts, folders, SMTP, SNMP, reporting and daily operations.

These editions share the same content structure. Screenshots show the real application using synthetic demonstration data only. No customer data or working passwords are displayed.

Contents

Essentials and installation

Architecture and responsibilities 3
Preparation and permissions 4
Install or upgrade an existing environment 5
Reading the client overview 6

Scenario 1 - one account

Scenario 1: one account and one archive 7
Scenario 1: validating the first delivery 8

Scenario 2 - shared administration

Scenario 2: multiple archives, shared administration 9
Scenario 2: managing inheritance 10

Scenario 3 - isolated environments

Scenario 3: three fully isolated environments 11
Scenario 3: a client-specific identity as an alternative 12

Folders and integrations

Mapping additional source folders 13
Publishing the upload folder catalogue 14
Empty import folders and recovery 15

SMTP and daily reports

SMTP: central error notifications 16
SMTP: testing and assessing delivery 17
Daily reports and client-specific notifications 18

SNMP and Zabbix

Configuring SNMPv3 securely 19
SNMP: numeric OIDs 20
SNMP: status, activation and limitations 21
Zabbix: items and triggers 22

Support and recovery

Support and administration 23
Managing Windows services 24
Backup, recovery and removal 25
Troubleshooting systematically 26
Acceptance and daily operations 27

Architecture and responsibilities

Server Manager is the administrative interface. Each client has its own Windows service, AnnTac sign-in, upload root, configuration and status. Uploads continue when nobody is signed in to Windows.

AnnTac Uplink Server Monitoring is a separate service. It collects errors, sends daily reports and publishes central SNMP data. It remains available when a client service stops.

The Windows service account determines access to files and shares. The AnnTac account selects the receiving archive. SMTP and SNMP accounts are independent. Do not confuse these four identities.

The central monitoring service runs as LocalSystem. It can read protected client status and reporting history. Separate clients on one host therefore do not form a hard security boundary against local administrators or LocalSystem.

Preparation and permissions

Install as a local administrator. Use a supported Windows x64 environment and test on the Windows Server version deployed at the customer. The installer contains the application; customers do not need Python, Inno Setup or SafeNet.

The upload service account requires Log on as a service. Uplink grants this locally during account configuration; domain policy can override it. Grant NTFS Modify on the upload root, source folders and their children: reading, writing, renaming and deleting are required.

Network sources require both share and NTFS permissions. Use UNC paths such as \\fileserver\exports\client-a. Do not use a user-mapped Z: drive. LocalSystem normally uses the computer identity for network access; a domain service account or gMSA is often more appropriate.

Allow outbound HTTPS to the AnnTac upload server and downloads.anntac.eu. Allow the selected SMTP port. Permit inbound SNMP UDP only from the monitoring server. Check DNS, proxy and certificate trust under the actual service identity.

Install or upgrade an existing environment

1. Keep the previous installer and back up configuration and document folders. Stop the old uploader, including desktop applications or scheduled tasks.

2. Run the signed installer as an administrator. The wizard follows the Windows interface language. Select the application language on the Taal / Language page; there is no separate language popup.

3. During an upgrade, select the existing AnnTac folder, for example D:\AnnTac. Existing Upload Folders, FTPS\Out categories and backups are reused in place. Do not select a new empty folder when existing documents must be retained.

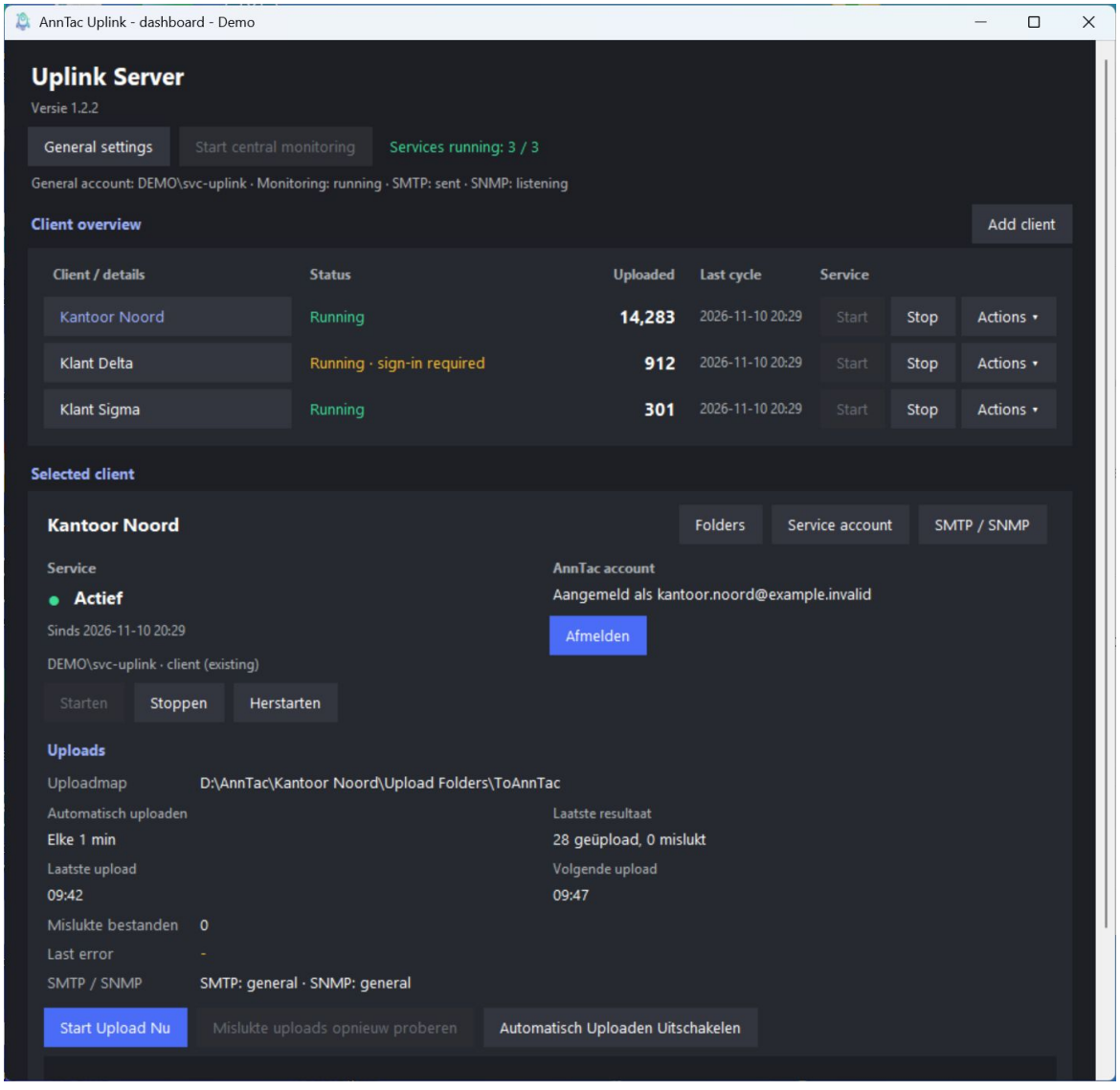
4. Setup stops services and leftover Uplink processes. VCRUNTIME DLLs use version-aware replacement. Restart when Setup requests it; do not use Skip as a workaround for an incomplete installation. Afterwards, check every service and perform a test upload.

Reading the client overview

Each row shows a customer, current service/upload status, recorded successful document deliveries, the latest cycle and individual Start/Stop buttons. Select a customer name to view its details.

Click a client name: Selected client groups that client's service, AnnTac account and uploads. Folders, Service account and SMTP / SNMP apply to the displayed customer. Actions in a client row selects that customer and contains Rename client, Update folders and Remove client. Add client is next to Client overview.

The counter is local delivery history, not a live inventory of the archive. .dx_ profile sidecars do not count as successful documents. An unreadable counter must be investigated as unknown rather than interpreted as zero.



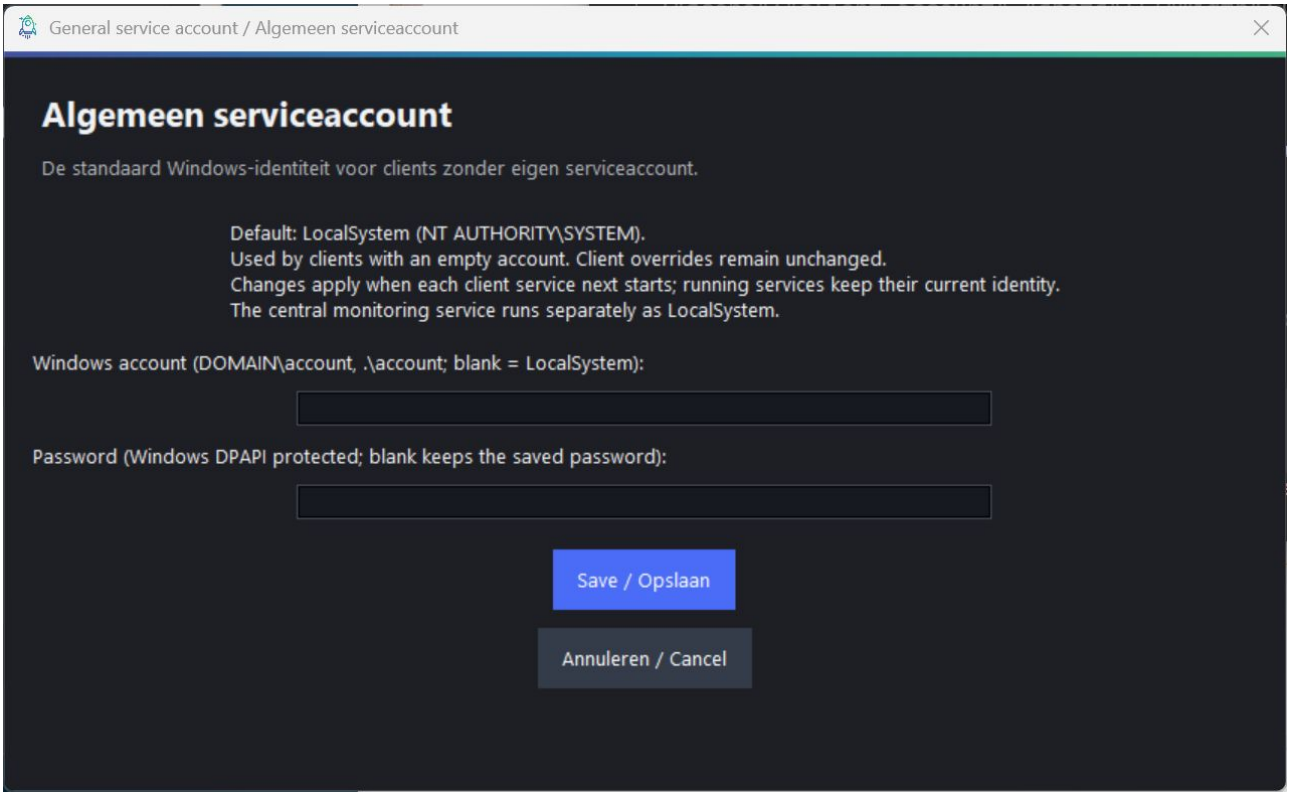
Application screenshot with demonstration data

Scenario 1: one account and one archive

Goal: one Windows installation, one AnnTac sign-in and one upload root. Use the original client and give it a recognisable customer name. Leave its service account empty to inherit the general setting.

Without a general account, the default is LocalSystem (NT AUTHORITY\SYSTEM). This normally works for local files. Shares may require a domain account. LocalSystem is not the AnnTac user and does not select the destination archive.

Sign in the client, confirm the activation email, verify the archive and upload one recognisable test document. Restart the service and Windows to verify uploads continue without an interactive login.



Application screenshot with demonstration data

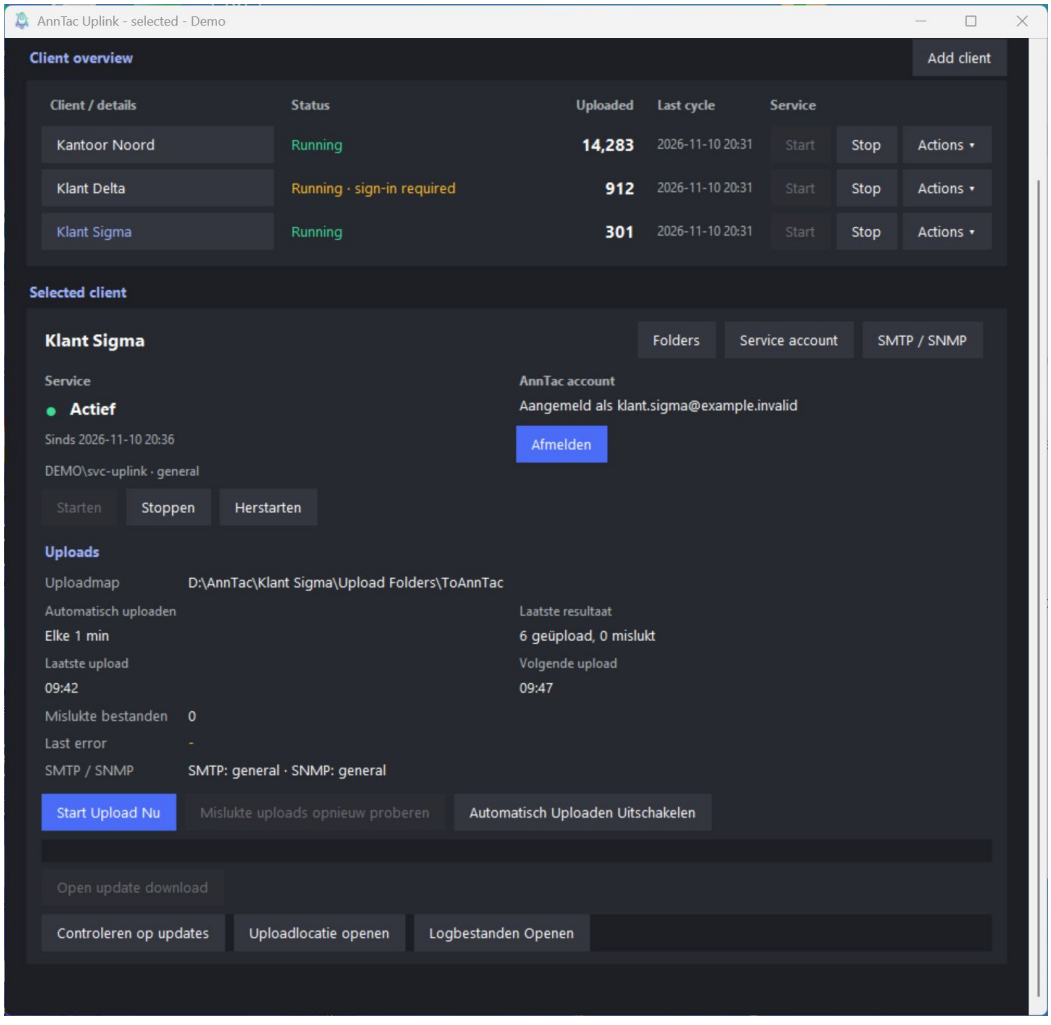
Scenario 1: validating the first delivery

Place a completed test document in a created top-level category, for example Upload Folders\ToAnnTac. Allow the producer to finish writing. Automatic processing applies a safety delay to recent or locked files.

Check, in order: service running, server reachable, account activated, scheduling enabled, latest result and the document in the correct AnnTac archive. Also test a subfolder and a document with a profile sidecar if the integration uses one.

Stopping a service does not sign out. Use Sign Out only when intentionally deactivating the backend session. Preserve source files and transfer journals after an error until delivery has been checked.

General settings, central monitoring and the running client-service count are at the top. The selected customer is named above its account and upload panel. Selecting a client displays its upload details; it does not automatically start an upload.



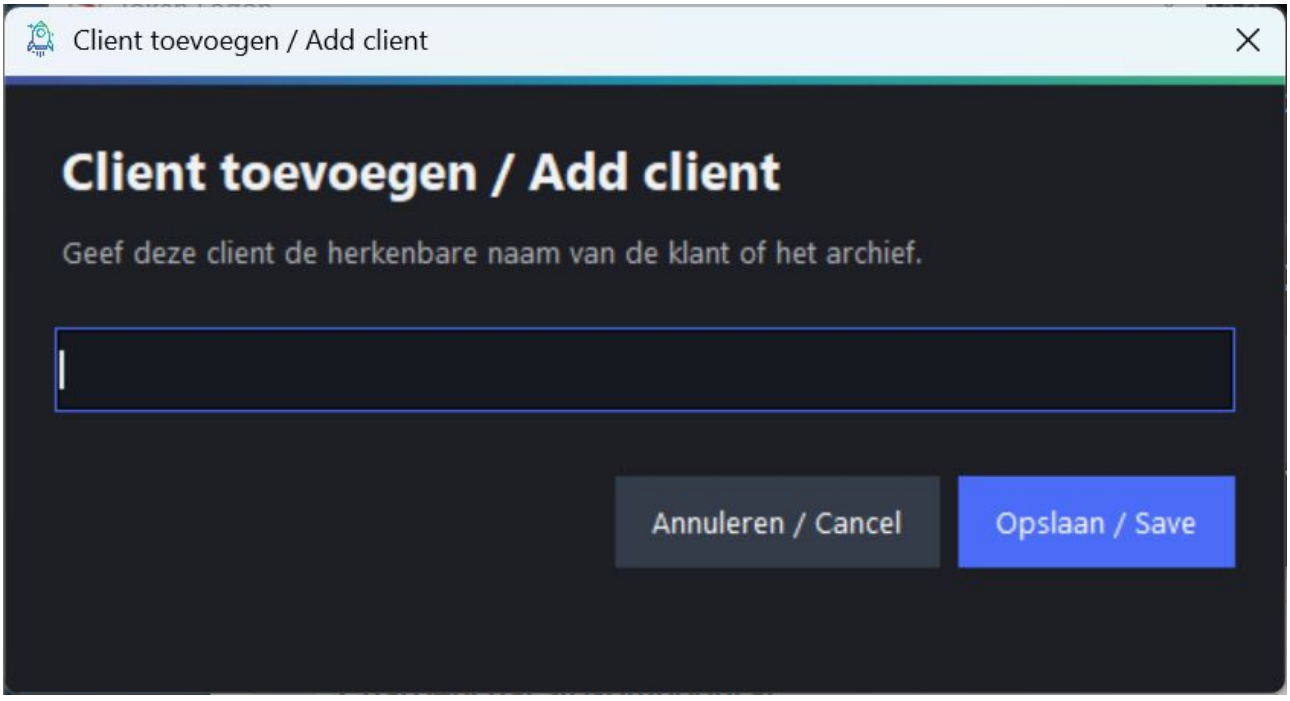
Application screenshot with demonstration data

Scenario 2: multiple archives, shared administration

Create a separate client for each customer archive. Each client receives its own AnnTac sign-in and a non-overlapping upload root. For example, use D:\AnnTac\CustomerA and D:\AnnTac\CustomerB; never configure two uploaders for the same source or upload folder.

Configure one general Windows service account and leave client account fields empty. Grant that account only the permissions required on the intended customer folders. Configure one general SMTP and SNMP policy for the IT provider.

The central monitoring service collects errors from every client. A client may additionally have its own notifications or report recipients. Test with different documents to verify each client delivers only to its intended archive.



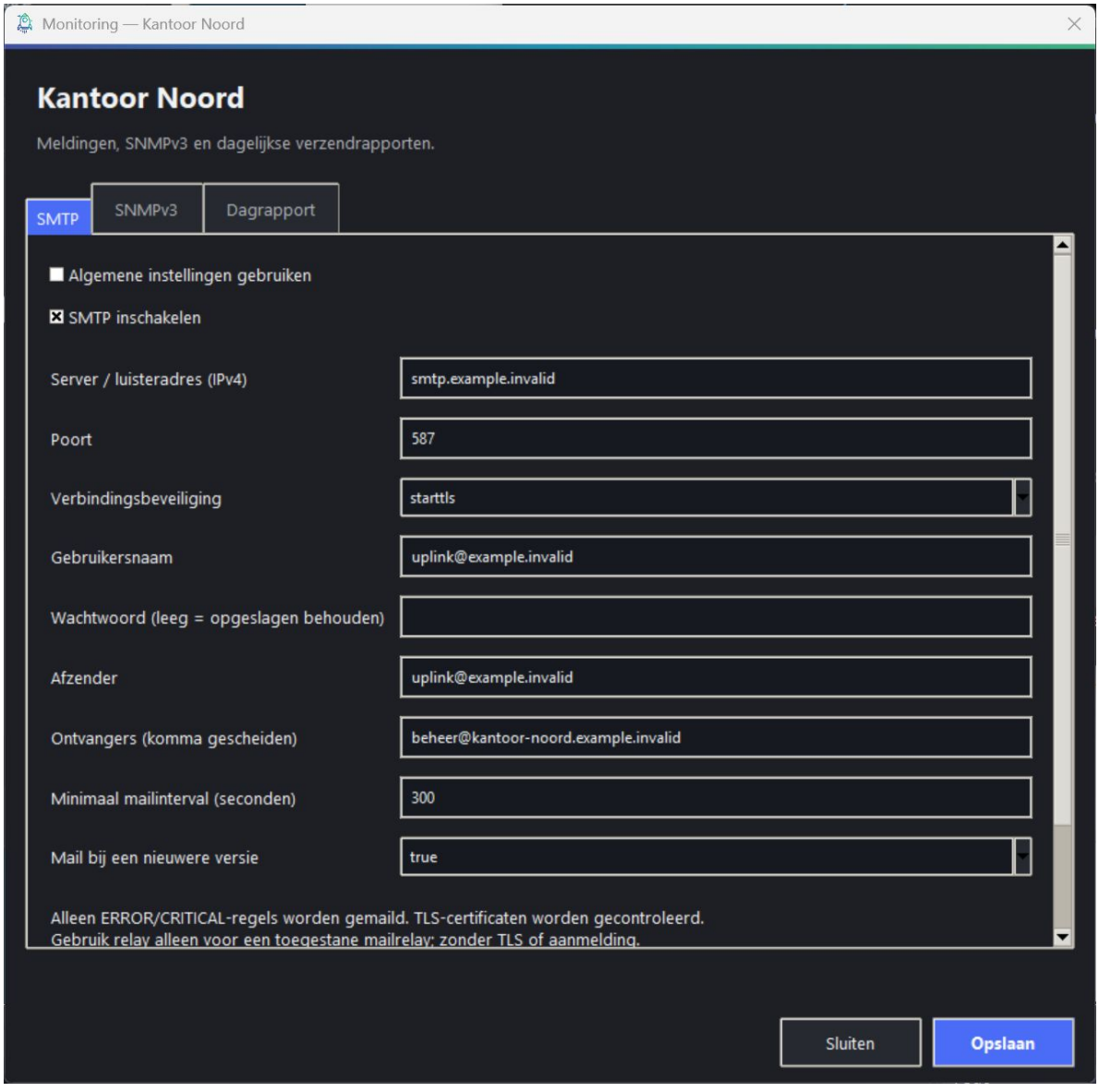
Application screenshot with demonstration data

Scenario 2: managing inheritance

General settings provide the defaults. For SMTP, SNMP and daily reports, Use general settings controls inheritance separately for each component. Clearing it enables an explicit client override.

An empty service account inherits the general account. A filled client account takes precedence. Existing explicit accounts from older installations are retained. Saving a general account updates Windows configuration for the next start; a running process changes identity only after stop/start.

Manager displays the actual identity of an active service and, when applicable, its next identity. The central monitoring service continues to run separately as LocalSystem.



Application screenshot with demonstration data

Scenario 3: three fully isolated environments

For full isolation, use three separate Windows instances, for example VM-A, VM-B and VM-C. Install Uplink separately on each VM, with its own service identity, AnnTac sign-in, document storage and local configuration.

Use separate SMTP/SNMP credentials and firewall rules for each environment. Do not grant a service account access to another environment's document or configuration folders. Backups and recovery procedures must also remain separate.

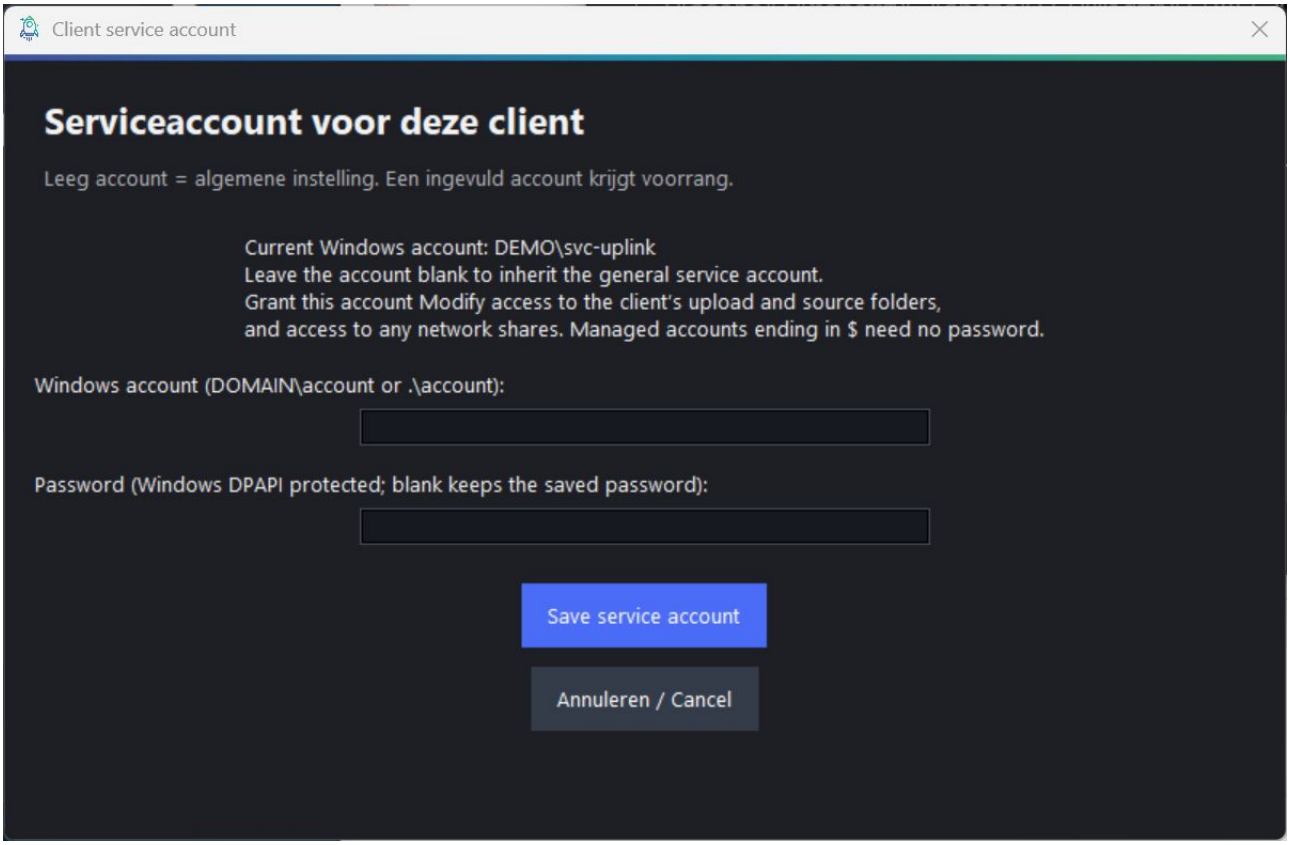
One external Zabbix system may monitor the three servers through three separate SNMP interfaces. This shares monitoring, not upload processes or sign-in tokens.

Three clients with different accounts on one host provide logical separation, not complete host isolation. The local administrator and central LocalSystem service can still access all client configuration on that host.

Scenario 3: a client-specific identity as an alternative

If deliberately sharing one host, configure a separate service account and separate source/upload folders per client. Stop the client before changing its identity. Enter DOMAIN\account, .\account or a provisioned gMSA.

Grant Modify on that client's document folders and appropriate share permissions for network sources. Uplink grants access to the client's protected configuration. A gMSA must be provisioned on the host first; a name ending in $ alone does not create a working gMSA.



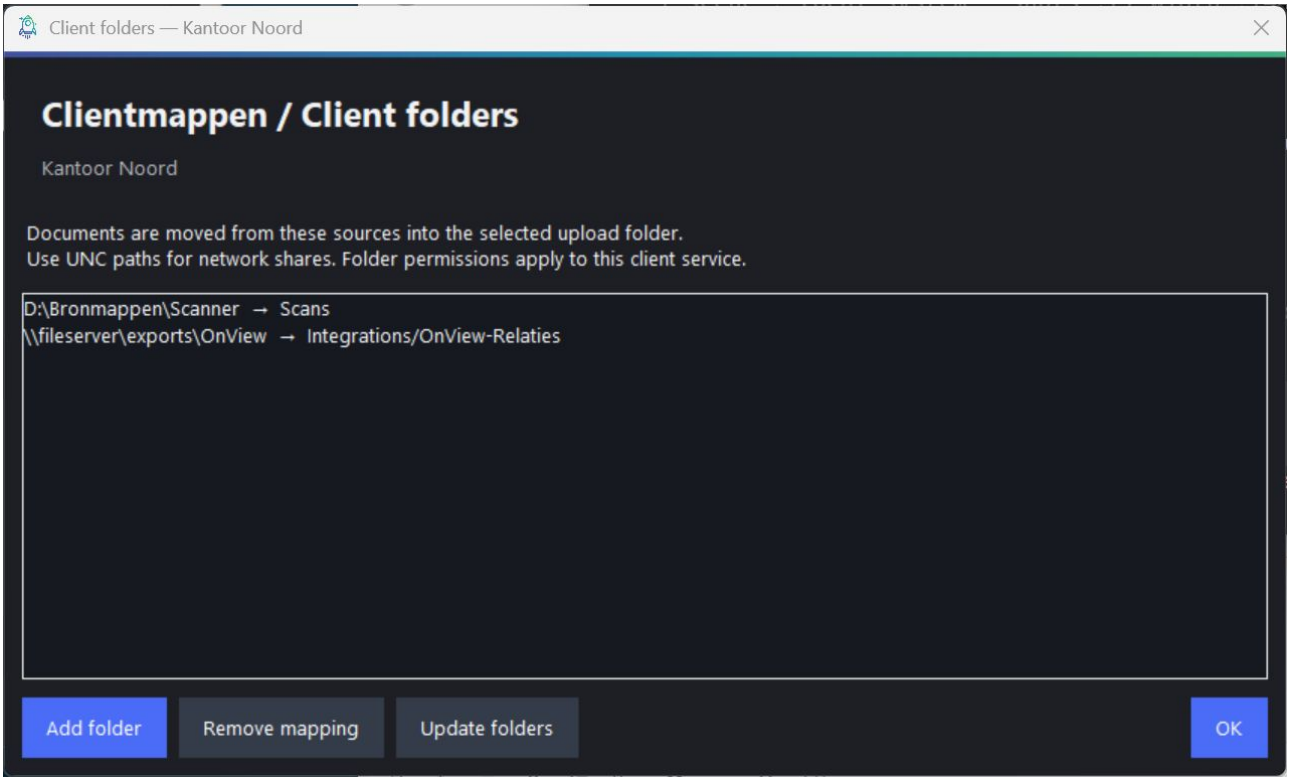
Application screenshot with demonstration data

Mapping additional source folders

Select the intended client and choose Folders. Add folder requests an existing source folder and then an upload category or integration. Use a UNC path for a share. Verify the selected client before saving.

Documents are transferred to an Imported-<mapping-id> subfolder within the destination category. The copy is verified before the original is removed. Removing a mapping stops future scans; already published or journalled transfers remain recoverable.

The OK button closes the dialog. The cleanup function does not delete the external source folder.



Application screenshot with demonstration data

Publishing the upload folder catalogue

AnnTac maintains the central upload folder catalogue. Update folders retrieves the current layout. Administrators do not need to configure an internal address.

Examples: Upload Folders\Scans; Upload Folders\ToAnnTac; Upload Folders\Integrations\Stratech; Upload Folders\Integrations\AnnTac_List_Converter. The list defines the folder layout; creating a folder does not implement new conversion or product logic.

Update folders fetches the list, creates missing folders and removes retired folders only when empty. Active mappings and incomplete transfer journals are protected. Non-empty old categories remain available for processing.

An unavailable or invalid list leaves the last known-good configuration intact. A new installation includes a fallback catalogue. Paths outside Upload Folders, unsafe names and traversal paths are rejected.

Empty import folders and recovery

After upload cycles, Uplink removes empty descendant folders, including Imported-… folders. Top-level categories and explicit integration paths from the catalogue remain, even when empty.

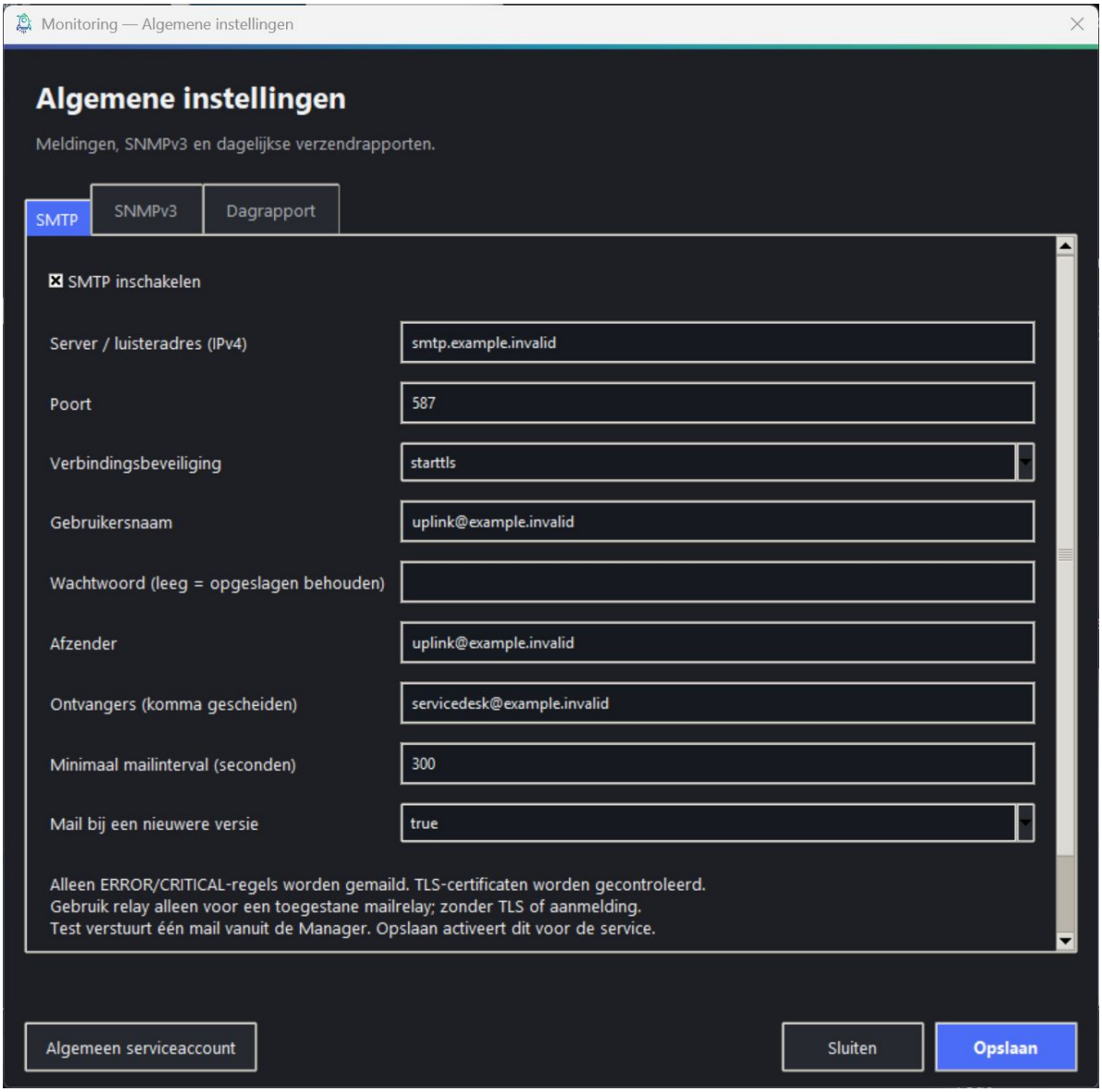
A folder opened by Explorer or another process may remain locked. Cleanup skips it and retries during a later cycle. It never deletes files for this purpose and does not follow symbolic links or junctions.

After an error, check the source, destination and imports.json before manually deleting anything. Existing destinations are not overwritten. Restore permissions or resolve the naming conflict and allow the next cycle to retry.

SMTP: central error notifications

Open General settings, SMTP tab. Enter the host, port, security mode, sender and recipients. Separate multiple recipients with commas. STARTTLS commonly uses port 587; implicit TLS commonly uses 465.

Relay is intended only for an explicitly authorised mail relay without TLS or login. Username/password authentication requires TLS. Certificate validation is not disabled.



Application screenshot with demonstration data

SMTP: testing and assessing delivery

Send test email sends one identifiable message from Manager. Save makes the service reload configuration. Also verify a real error notification: Manager and LocalSystem/service accounts may have different network, proxy or relay permissions.

Normal error email contains ERROR/CRITICAL records; successful uploads and ordinary warnings are not emailed. Central delivery batches errors and acknowledges journals only after SMTP acceptance. The default minimum interval is 300 seconds.

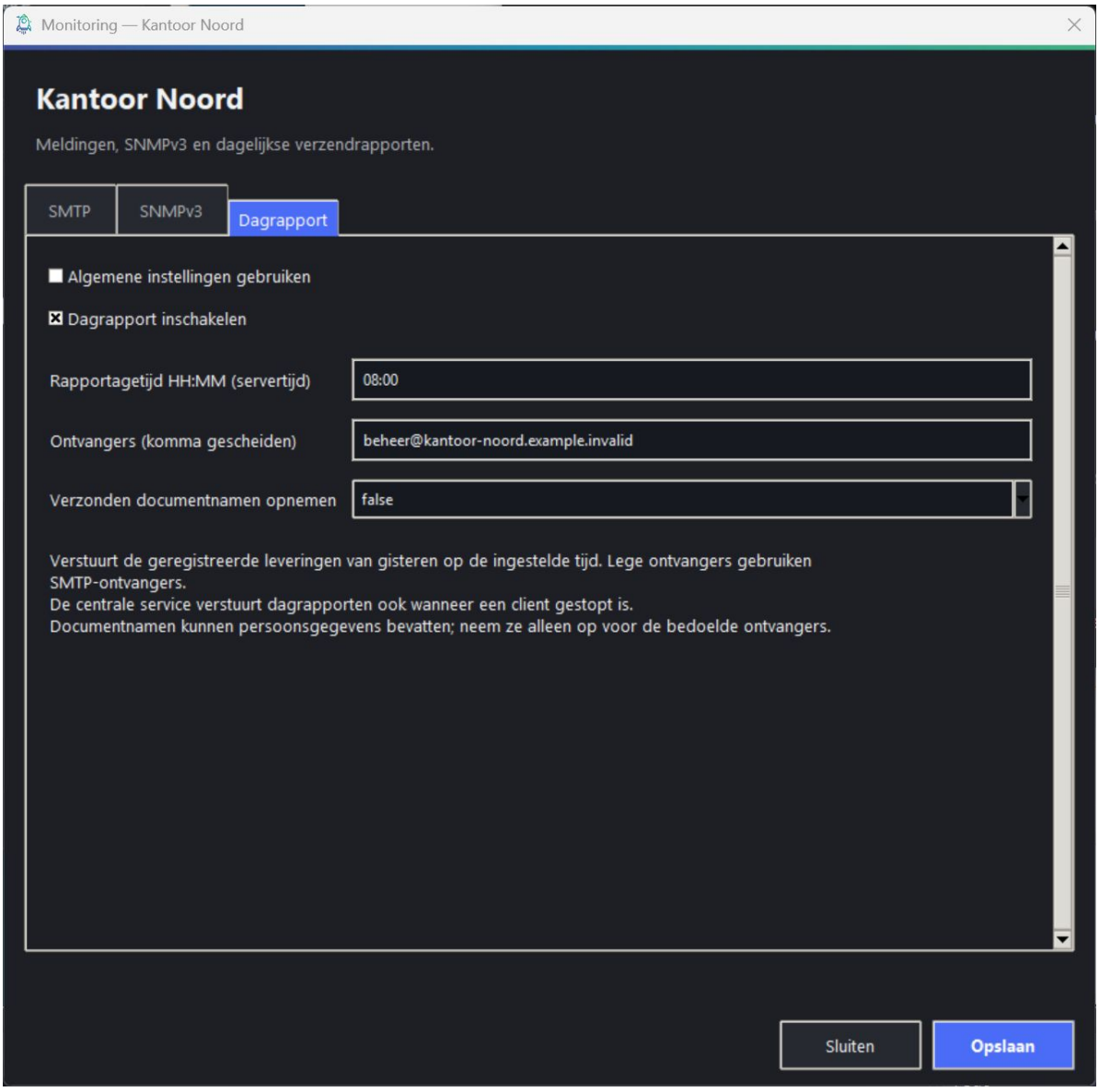
SMTP acceptance does not prove final mailbox delivery. If a message is missing, also check quarantine, spam filtering and bounces. A crash between acceptance and local acknowledgement may produce a duplicate.

Passwords are machine-bound using Windows DPAPI. An empty password field retains the saved value. Re-enter monitoring passwords on a new server; never share tokens, PINs or passwords in support tickets.

Daily reports and client-specific notifications

On the client, open Monitoring, Daily report tab. Configure enabled/disabled, a local server time and optional recipients. Empty recipients use the effective SMTP recipients. Reports cover the previous calendar day.

The report includes recorded successful documents, failed file attempts and cycles. Document names are optional and disabled by default. History starts with this feature, is retained for 90 days and is not reconstructed from the archive.

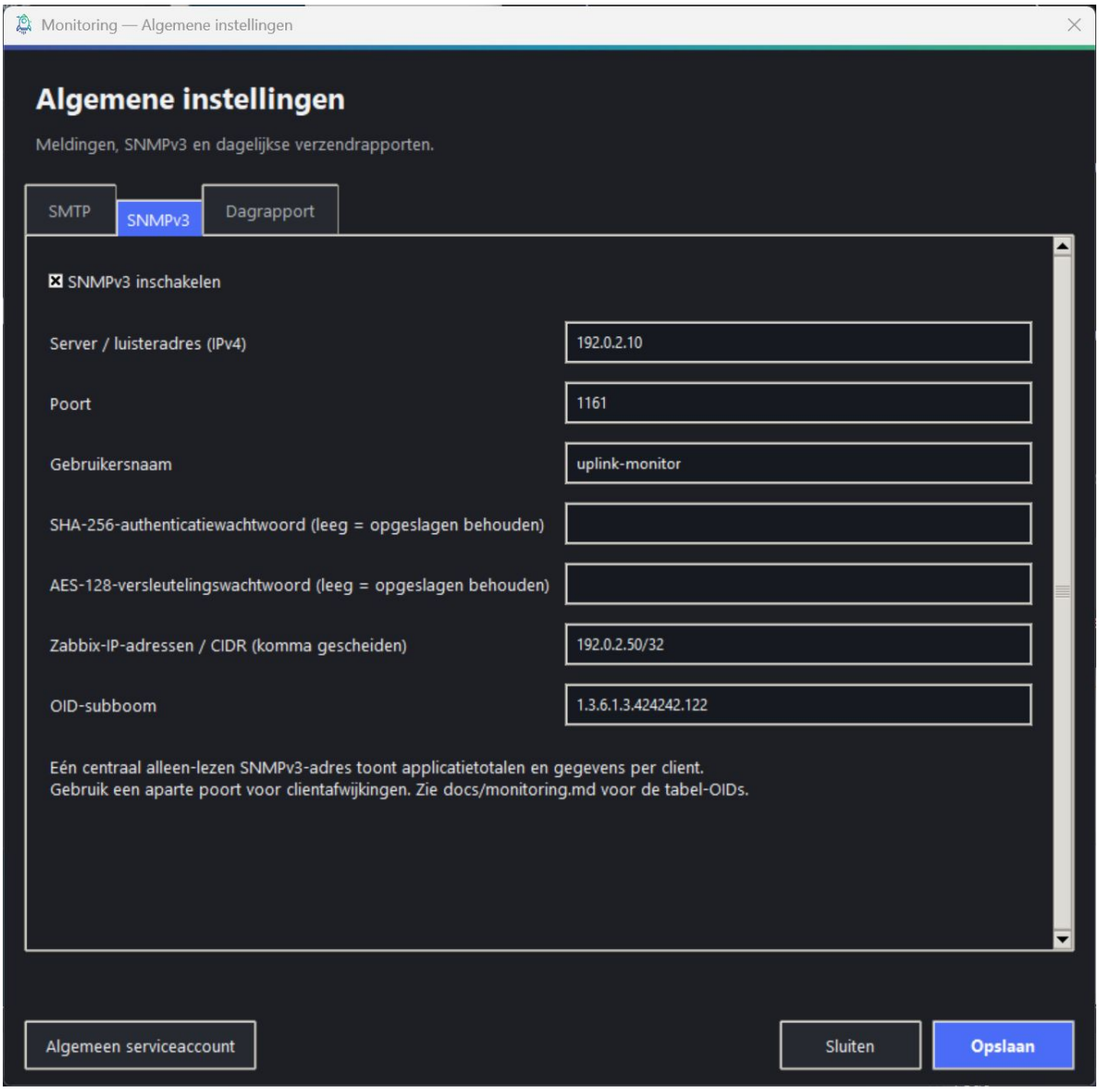


Application screenshot with demonstration data

Configuring SNMPv3 securely

Enable general SNMP and select the server's actual IPv4 listening address. 127.0.0.1 is local only. For example, use UDP 1161 and restrict both the allowlist and firewall to the monitoring server.

Use SNMPv3 authPriv, SHA-256 and AES-128 with a dedicated username and two passwords of at least eight characters. There is no unsecured SNMPv1/v2c community. A client-specific listener requires a different port.



Application screenshot with demonstration data

SNMP: numeric OIDs

B is the configured base OID. The built-in base 1.3.6.1.3.424242.122 is experimental, not a registered AnnTac PEN. For a formal enterprise MIB, use a subtree assigned to your organisation.

B.M.0 is a scalar. Central client rows use B.100.I.M.0, where I is the stable row index and M the metric number. Discover rows using GETNEXT/GETBULK; metric 24 returns the client ID and 25 the customer name.

1 version; 2 state; 3 heartbeat age; 4 server reachable; 5 authentication valid; 6 scheduling enabled; 7 failed files; 8 last cycle successful; 9 last cycle failed; 10 total successful; 11 total failed attempts; 12 error counter; 13 last error; 14 error time (Unix); 15 last action; 16 action time (Unix).

SNMP: status, activation and limitations

17 SMTP state; 18 uptime; 19 update available; 20 health (1 healthy, 2 attention); 21 last cycle time; 22 statistics valid; 23 last error-email time; 24 client ID; 25 customer name; 26 Windows startup type (2 automatic, 3 manual, 4 disabled, 0 unknown).

The endpoint is read-only: GET, GETNEXT and GETBULK. There is no SET, remote start/stop or traps. Also monitor missing data/timeouts: a stopped monitoring service cannot report itself. Central totals may decrease when a client is removed; use client rows for historical rates.

Non-applicable central fields are zero or empty. Use client rows for the last action/cycle. Heartbeats and counters are the latest published values, not an independent probe of the AnnTac server.

Zabbix: items and triggers

Create an SNMP interface using the server address, UDP port, authPriv, SHA256 and AES128. Use numeric OIDs; select Numeric unsigned for status/counters and Text for text fields. Labels vary between Zabbix versions.

Recommended triggers: no data for 3 minutes; heartbeat older than 60 seconds across multiple polls; server unreachable for 5 minutes; invalid authentication while the server is reachable; failed files > 0; increasing error counter; SMTP state starts with failed.

Use B.100.I.26.0 to recognise deliberately disabled client services. Account for maintenance agreements and counter resets after a restart.

Example: snmpget -v3 -l authPriv -u uplink-monitor -a SHA-256 -x AES -A <auth-key> -X <privacy-key> <server>:1161 1.3.6.1.3.424242.122.1.0. Store real secrets in secure monitoring configuration, not support tickets or shared command history.

Support and administration

AnnTac ensures customers receive the current release. Use the installer supplied by AnnTac or your IT administrator.

For an incident, contact your IT administrator or AnnTac. Include the client name, time and visible error message. Do not share passwords or access tokens.

Managing Windows services

In services.msc, customer services are named AnnTac Uplink Server - Customer name. Internal IDs remain AnnTacUplink for the original client and AnnTacUplink-client-... for added clients. The central ID is AnnTacUplink-monitor. Renaming a customer does not change its internal ID.

Upgrades retain Disabled startup mode. Restore Manual or Automatic before starting that client again. Stopping one customer does not stop other customers or central monitoring.

Backup, recovery and removal

Keep the installer, client inventory, upload locations, service identities and a consistent backup of %ProgramData%\AnnTac Uplink plus document/backup folders. Stop services or use a consistent backup method before copying configuration and transfer journals.

Protect user.ini, accounts.json, global/settings.ini, transfer journals, monitoring state and report history. Tokens and machine-bound encrypted secrets must not be placed in public tickets. Re-enter monitoring and account passwords on a new machine.

Remove client stops and deletes the selected service and registration. Documents, sources, backups and saved settings remain for recovery. Handle retained credentials according to your retention policy.

Uninstalling is different: the existing uninstaller removes services and protected configuration. Documents outside that configuration directory remain. Verify backups before uninstalling and always test delivery to the correct archive after recovery.

Troubleshooting systematically

No uploads: check the service, server reachability, activation, scheduling, file readiness and folder permissions in that order. A running service does not prove a valid AnnTac session or access to the share.

Access denied: check the actual service identity, NTFS and share permissions, and Log on as a service. Test UNC access under that identity. Also check domain policy and an expired service password.

No email: check host/port, TLS, credentials, relay policy, firewall, quarantine and spam filtering. No SNMP: check the central service, binding address, unique port, firewall, allowlist and matching SHA256/AES128 keys.

Empty folder remains: close Explorer/the producer and allow a later cycle to clean it up. Files remain: inspect client logs, last_error and the transfer journal. Do not delete a source or journal before checking the destination.

Text logs switch to a new file daily using the UTC date. While running, Uplink checks every minute for logs that have not been modified for more than 90 days and attempts to remove them. Locked files are retried later. There is no fixed maximum daily file size. Error journals have a 90-day retention period; document backups use a separate configurable period.

Acceptance and daily operations

Before rollout: test an upgrade using the old AnnTac root; a fresh installation; the reported runtime-DLL reinstall case; local and UNC sources; a profile sidecar; a locked file; a network outage; service restart and reboot.

Scenario 1: verify LocalSystem or the selected account and one correct archive. Scenario 2: test every sign-in and central/client notifications. Scenario 3: demonstrate that VM-A identities cannot access VM-B/VM-C.

Test Update folders with a new integration folder, an empty retired folder and a non-empty retired folder. Test cleanup while a folder is open.

Daily: check central health, inactive accounts, errors, remaining documents, email delivery and backup results. Periodically: perform a restore test, review permissions and service accounts, and record changes.

This guide describes the Uplink Server interface. Screenshots are real renders with demo data. Regression tests and signing do not replace acceptance testing on the customer server.