UNITED SECURITY PROVIDERS

USP Network Authentication System®

Migration Guide

Version 16.0

United Security Providers AG
www.united-security-providers.ch
info@united-security-providers.ch

Headquarter Stauffacherstrasse 65/15 CH-3014 Bern Tel. +41 31 959 02 02
Baslerpark Mürtschenstrasse 27 CH-8048 Zürich Tel. +41 44 496 61 11

UNITED SECURITY PROVIDERS

UNITED SECURITY PROVIDERS

Contents

1 USP NAS 16.0

1.1 Summary

This migration guide provides a set of guidelines to migrate the USP Network Authentication System® from versions 15.x to the latest version 16.0.

In most cases, no actions are required and all changes are done automatically. However, some minor manual changes might be required by the update. Consult the migration guide carefully prior the update and apply any steps required before or after the update.

When upgrading existing installations, please follow the recommended upgrade procedure outlined in the "USP NAS Installation Guide".

If you are updating from a Network Authentication System® Appliance older than version 15.0, please consult also the migration guides for all intermediate versions, as this migration guide only outlines the changes between the new and the previous USP Network Authentication System® version.

1.2 Changes in the REST API

The naming in the data structure of the **netdevices**, **interfaces** and **endpoints REST APIs** has been standardized. All property names and filter parameters are now written in **camel case** instead of a mix of snake case and camel case. For example, a property like **netdevice_id** has been renamed to **netdeviceId**.

Additionally, many more properties and filter parameters have been added, and the performance with large data sets has been improved. Properties are now also ordered in a more logical way.

Please consult the online REST API documentation in the USP NAS Web GUI for mode details.

Here are some examples on the differences in the REST API response between release 15.x and 16.0:

1.2.1 Netdevices

Version 15.4

```
[
  {
    "id": 1002004,
    "device_name": "cisco-c-1300",
    "device_ip": "10.15.1.20",
    "device_class": "SWITCH",
    "portgroups": [
        "Main building"
    ],
    "errorcode": 0,
    "source": "testlab",
    "inscope": 1,
    "updated": "2025-08-21T12 ↩
    :08:50.574+00:00",
    "created": "2025-08-21T12 ↩
    :01:48.442+00:00",
    "location": "Datacenter East",
    "devicetype": " ↩
    GenericQBridgeMibAdaptor",
    "description": "Catalyst 1300  ↩
    Series Managed Switch (C1300-8P-E-2G)",
    "snmpAccessProfileId": "52f36b8b-4 ↩
    d6c-45b1-80b9-3c2cb4852073",
    "snmpAccessProfileName": null,
    "snmpVersion": "SNMPV3",
    "snmpAuthenticationAlgorithm": " ↩
    SHA512",
    "snmpEncryptionAlgorithm": "AES128"
  }
]
```

Version 16.0

```
[
  {
    "id": 1002004,
    "deviceName": "cisco-c-1300",
    "deviceIp": "10.15.1.20",
    "deviceClass": "SWITCH",
    "deviceType": " ↩
    GenericQBridgeMibAdaptor",
    "inScope": "IN_SCOPE",
    "location": "Datacenter East",
    "description": "Catalyst 1300  ↩
    Series Managed Switch (C1300-8P-E-2G)",
    "accessControl": "SYSTEMDEFAULT",
    "accounting": " ↩
    ACCOUNTING_ENABLED_ALL",
    "snmpAccessProfileId": "52f36b8b-4 ↩
    d6c-45b1-80b9-3c2cb4852073",
    "snmpAccessProfileName": null,
    "snmpVersion": "SNMPV3",
    "snmpAuthenticationAlgorithm": " ↩
    SHA512",
    "snmpEncryptionAlgorithm": "AES128 ↩
    ",
    "errorCode": "NO_ERROR",
    "portGroup": "Main building",
    "accessRule": "BASEACCESSRULE",
    "accessMode": "RESTRICTIVE",
    "hasNetports": true,
    "source": "testlab",
    "created": "2025-08-21T12:01:48.442 ↩
    Z",
    "updated": "2025-08-21T12:25:52.539 ↩
    Z",
    "lastScan": "2025-08-21T12 ↩
    :25:52.529Z"
  }
]
```

- Previously, the response contained an array `portgroups` for the assigned portgroups. It has been replaced with a property `portGroup` indicating the effective portgroup in use, based on its priority.
- New properties `accessControl`, `accounting`, `accessRule`, `accessMode`, `hasNetports`, `lastScan` have been added.
- New filters for `description`, `accessControl`, `snmpAccessProfileName`, `portGroup`, `accessRule`, `hasNetports`, `lastScan` have been added.
- Numeric values of properties `errorCode` and `inScope` have been replaced with a descriptive name. This also affects the respective filters.

1.2.2 Interfaces

Version 15.4

```
[
  {
    "id": 1002231,
    "netdevice_id": 1002004,
    "portgroups": [
      "Main building"
    ],
    "ifname": "gi1",
    "ifindex": 1,
    "ifalias": "uplink",
    "dot1xstate": 1,
    "defaultvlan": 1,
    "netport": true
  },
  {
    "id": 1002232,
    "netdevice_id": 1002004,
    "portgroups": [
      "Main building"
    ],
    "ifname": "gi2",
    "ifindex": 2,
    "ifalias": "access",
    "dot1xstate": 0,
    "defaultvlan": 1,
    "netport": false
  }
]
```

Version 16.0

```
[
  {
    "id": 1002231,
    "netdeviceId": 1002004,
    "netdeviceName": "cisco-c-1300",
    "netdeviceIp": "10.15.1.20",
    "ifName": "gi1",
    "ifIndex": 1,
    "ifAlias": "uplink",
    "nodeCount": 14,
    "dot1xEnabled": false,
    "defaultVlan": 1,
    "netportType": "NETPORT",
    "portGroup": "Main building",
    "accessRule": "BASEACCESSRULE",
    "accessMode": "RESTRICTIVE",
    "updated": "2025-08-21T13 ↩
    :07:44.441327Z"
  },
  {
    "id": 1002232,
    "netdeviceId": 1002004,
    "netdeviceName": "cisco-c-1300",
    "netdeviceIp": "10.15.1.20",
    "ifName": "gi2",
    "ifIndex": 2,
    "ifAlias": "access",
    "nodeCount": 0,
    "dot1xEnabled": true,
    "defaultVlan": 1,
    "netportType": null,
    "portGroup": "Main building",
    "accessRule": "BASEACCESSRULE",
    "accessMode": "RESTRICTIVE",
    "updated": "2025-08-21T13 ↩
    :07:44.441327Z"
  }
]
```

- Previously, the response contained an array `portgroups` for the assigned portgroups. It has been replaced with a property `portGroup` indicating the effective portgroup in use, based on its priority.
- New properties `netdeviceName`, `netdeviceIp`, `nodeCount`, `accessRule`, `accessMode`, `updated` have been added.
- Numeric property `dot1xstate` has been replaced with boolean property `dot1xEnabled`.
- Boolean property `netport` has been replaced with property `netportType` since there exist more than one netport types. A value of `null` indicates that no netport of any kind is configured.
- New filters for `netdeviceName`, `netdeviceIp`, `dot1xEnabled`, `defaultVlan`, `isNetport`, `portGroup`, `accessRule` have been added.

1.2.3 Endpoints

Version 15.4


```
[
  {
    "macAddress": "00012e703675",
    "macVendor": "PC Partner Ltd.",
    "status": "ACTIVE",
    "netdevice_id": 1002000,
    "ifname": "gi8",
    "ifindex": 8,
    "ifalias": "8021x",
    "vlan": 1,
    "defaultvlan": 1,
    "clientip": "192.168.100.53",
    "clientip_updated": "2025-08-21T12 ↩
    :25:33.360+00:00",
    "client_router_name": "fortigate-80 ↩
    e",
    "client_router_ip":  ↩
    "192.168.100.99",
    "clientname": null,
    "clientname_inventory": null,
    "eap_username": "host/zotac-zbox",
    "eap_username_inventory": "zotac- ↩
    zbox",
    "location": null,
    "source": "EAP_CACHE",
    "changedBy": null,
    "inventoried": true,
    "assetId": "n/a",
    "assettype": null,
    "assetclass": null,
    "lastcheck": "2025-08-21T12 ↩
    :23:40.231+00:00",
    "updated": "2025-08-21T12 ↩
    :25:34.140+00:00",
    "created": "2025-08-21T12 ↩
    :02:35.922+00:00",
    "devicename": "cisco-cbs-250",
    "deviceip": "192.168.100.100",
    "portGroup": "Global",
    "accessMode": "ALLOWED",
    "accessRule": "BASEACCESSRULE",
    "endpointDetails": [
      {
        "source": "EAP",
        "key": "subject.commonName",
        "value": "zotac-zbox"
      }
    ]
  }
]
```


Version 16.0


```
[
  {
    "macAddress": "00012e703675",
    "macVendor": "PC Partner Ltd.",
    "eapUsername": "host/zotac-zbox",
    "clientIp": "192.168.100.53",
    "clientIpUpdated": "2025-08-21T12 ↩
    :25:33.360Z",
    "clientNameDns": null,
    "vlan": 1,
    "status": "ACTIVE",
    "authType": "IEEE802DOT1X",
    "firstSeen": "2025-08-21T12 ↩
    :02:35.922Z",
    "lastSeen": "2025-08-21T13 ↩
    :07:26.915Z",
    "lastCheck": "2025-08-21T12 ↩
    :23:40.231Z",
    "lastEvent": "2025-08-21T12 ↩
    :23:40.243Z",
    "lastStatusChange": "2025-08-21T12 ↩
    :23:40.227089Z",
    "netdeviceId": 1002000,
    "netdeviceName": "cisco-cbs-250",
    "netdeviceIp": "192.168.100.100",
    "ifName": "gi8",
    "ifIndex": 8,
    "ifAlias": "8021x",
    "defaultVlan": 1,
    "portGroup": "Global",
    "accessRule": "BASEACCESSRULE",
    "accessMode": "ALLOWED",
    "routerName": "fortigate-80e",
    "routerIp": "192.168.100.99",
    "inventoried": true,
    "authorized": true,
    "identityType": "EAP_LAN",
    "eapUsernameInventory": "zotac-zbox ↩
    ",
    "clientNameInventory": null,
    "location": null,
    "owner": null,
    "assetType": null,
    "assetClass": null,
    "tenant": null,
    "doubleAttached": false,
    "assetId": null,
    "changedBy": null,
    "source": "EAP_CACHE",
    "inventoryCreated": "2025-08-21T12 ↩
    :23:40.221Z",
    "inventoryUpdated": "2025-08-21T12 ↩
    :23:40.221Z",
    "inventoryValidUntil": null,
    "endpointDetails": [
      {
        "source": "EAP",
        "key": "issuer.commonName",
        "value": "ca.test.usp-nas. ↩
    internal"
      }
    ]
  }
]
```

Version 15.4	Version 16.0

- Properties have been ordered according to *Node in network* → *Netdevice* → *Inventory record*.
- New properties `authType`, `lastEvent`, `lastStatusChange`, `authorized`, `identityType`, `owner`, `tenant`, `doubleAttached`, `inventoryCreated`, `inventoryUpdated`, `inventoryValidUntil` have been added.
- `clientname` has been renamed to `clientNameDns`.
- `client_router_name` and `client_router_ip` have been renamed to `routerName` and `routerIp` respectively.
- `created` has been renamed to `firstSeen`, and `updated` has been renamed to `lastSeen`.
- New filters have been added for almost all properties.
- Filters for `eapUsername` and `clientName` now check both network and inventory record.
- If a netdevice has been deleted, the related values will be set to `null`.

1.3 Migration of SAB functionality to Java

Backup-related functionality of the SAB CLI API tool has been migrated into the USP NAS core daemon Java code. As a consequence the following SAB function can no longer be used directly on the CLI:

```
sab backup:set_backup
sab backup:get_backup
sab backup:del_backup
sab backup:run_backup
sab backup:do_backup
sab backup:do_validate
sab backup:do_restore
```

1.4 Deprecation notice

The following functionality is considered deprecated/obsolete and will be removed or replaced with an alternative implementation in the next USP NAS major release 17.0:

- SNMP trap forwarder
- VLAN Zones/WLAN ACL Zones (to be replaced by new policy management implementation)
- Netdevice classes WTP/ACCOUNTING (to be replaced by new policy management implementation)
- Soft-deleted netdevices/netports
- Soft-deleted endpoints

2 USP NAS 15.0

2.1 Summary

This migration guide provides a set of guidelines to migrate the USP Network Authentication System® from versions prior to 14.0 to the latest version 15.0.

In most cases, no actions are required and all changes are done automatically. However, some minor manual changes might be required by the update. Consult the migration guide carefully prior the update and apply any steps required before or after the update.

When upgrading existing installations, please follow the recommended upgrade procedure outlined in the "USP NAS Installation Guide".

If you are updating from a Network Authentication System® Appliance older than version 14.0, please consult also the migration guides for all intermediate versions, as this migration guide only outlines the changes between the new and the previous USP Network Authentication System® version.

2.2 Introduction of SNMP Access Profiles

Starting from this release, SNMP access profiles are being used to store credentials for accessing switches and routers via SNMP for network mapping, monitoring and enforcement (if SNMP MAC authentication is used). SNMP access profiles define the SNMP version to be used as well as the read/write community (in case of Version 1 and 2) or username, passwords and encryption algorithms (in case of version 3). These profiles can be managed at a dedicated location in the WebGUI, and therefore SNMP credentials no longer have to be defined for each netdevice; an SNMP access profile must be chosen instead. Every netdevice which should be monitored by SNMP must be assigned an SNMP access profile. There is no default SNMP community/username/password settings anymore in the global configuration.

SNMP access profile can be given a unique name; if omitted, an auto-generated name based on the stored data is created.

Due to the redesigned user interface for managing these profiles, new SNMPv3 authentication and encryption algorithm combinations are now supported, which increase security and compatibility in communicating with your netdevices.

During USP NAS Appliance update, existing entries are migrated automatically, and SNMP access profiles are created as needed. This applies as well to netdevices which use the global configured credentials in the past.

CSV data imports make use of the new profiles as well: for each record in an import file, it is checked if a profile matching the provided data exists, and it is assigned, or a new profile will be created. Therefore, existing import mechanisms don't need to be adapted. Optional, named SNMP access profiles can be specified directly as a new column in the import file. Please see the dedicated data import specification document for details.

If you use **scheduled scripts** to create netdevice entries in the database, some manual changes might be needed. Please refer to the newly added scrip template `NetdeviceGenerater.jy` to see an example on how this can be used.

RADIUS subnet definitions make use of the new profiles too. This enables the possibility to auto-inventorize netdevices with SNMPv3 credentials configured.

2.3 Changes in the REST API

In the netdevice REST API, the query filter parameter `snmpVersion` has been replaced by `snmpAccessProfileId` which references the assigned SNMP access profile. The response will now contain the fields `snmpAccessProfileId`, `snmpAccessProfileName`, `snmpVersion` (which can now be `SNMPV1`, `SNMPV2C` or `snmpv3`), `snmpAuthenticationAlgorithm` and `snmpEncryptionAlgorithm`.

Therefore, a REST API response for netdevices, which previously looked like this:

```
{
    "id": 1055600,
    "device_name": "cisco250",
    "device_ip": "192.168.100.100",
    "device_class": "SWITCH",
    "errorcode": 0,
    "source": "WEBGUI",
    "inscope": 1,
    "updated": "2024-11-18T11:26:34.653+00:00",
    "created": "2024-11-18T11:24:53.841+00:00",
    "deleted": null,
    "location": "USP Lab",
    "snmpVersion": "V2C",
    "devicetype": "GenericQBridgeMibAdaptor",
    "description": "CBS250-8T-D 8-Port Gigabit Smart Switch"
},
{
    "id": 1056000,
    "device_name": "v3test",
    "device_ip": "1.2.3.4",
    "device_class": "SWITCH",
    "errorcode": null,
    "source": "WEBGUI",
    "inscope": 1,
    "updated": "2024-11-18T14:14:39.278+00:00",
    "created": "2024-11-18T14:14:39.278+00:00",
    "deleted": null,
    "location": null,
    "snmpVersion": "V3_PRIV_AES_SHA512",
    "devicetype": null,
    "description": null
}
```


will now look like in release 15.0:


```
{
    "id": 1086800,
    "device_name": "cisco250",
    "device_ip": "192.168.100.100",
    "device_class": "SWITCH",
    "errorcode": 0,
    "source": "WEBGUI",
    "inscope": 1,
    "updated": "2025-01-06T10:44:44.609+00:00",
    "created": "2025-01-06T07:24:01.525+00:00",
    "deleted": null,
    "location": "USP Lab",
    "devicetype": "GenericQBridgeMibAdaptor",
    "description": "CBS250-8T-D 8-Port Gigabit Smart Switch",
    "snmpAccessProfileId": "9b9f8e1e-2239-4599-8d36-94e5ffa3791e",
    "snmpAccessProfileName": "SNMPv2 default profile",
    "snmpVersion": "SNMPV2C",
    "snmpAuthenticationAlgorithm": null,
    "snmpEncryptionAlgorithm": null
```



```
},
{
    "id": 1089000,
    "device_name": "v3test",
    "device_ip": "1.2.3.4",
    "device_class": "SWITCH",
    "errorcode": 1,
    "source": "WEBGUI",
    "inscope": 1,
    "updated": "2025-01-06T10:46:04.034+00:00",
    "created": "2025-01-06T10:40:34.565+00:00",
    "deleted": null,
    "location": null,
    "devicetype": null,
    "description": null,
    "snmpAccessProfileId": "728500ae-e051-4ab2-a846-67b0f8acac63",
    "snmpAccessProfileName": "v3 Test Profile",
    "snmpVersion": "SNMPV3",
    "snmpAuthenticationAlgorithm": "SHA512",
    "snmpEncryptionAlgorithm": "AES128"
}
```


2.4 Migration of SAB functionality to Java

Some mail-related functionality of the SAB CLI API tool has been migrated into the USP NAS core daemon Java code. As a consequence the following SAB function can no longer be used in custom scripts to send emails:

```
sab monitoring:alerting:send_mail
sab tools:send_mail
```

2.4.1 Jython Script Mail Interface

Instead of using the SAB commandline tool, it is now possible to send mails using custom Jython scripts. The command for this is:

```
mail.sendMail(String recipient, String subject, String body)
mail.sendMail(String recipient, String subject, String body, String attachmentFilePath)
```

It will send a mail using the mail server settings configured in the GUI.

2.5 MobileIron integration removed

We removed support for the **MobileIron** MDM solution, a company and product which has been acquired by Ivanti and integrated into their "Ivanti Neurons for MDM" solution a few years ago. If by any chance you are still using MobileIron in connection with USP NAS to obtain endpoint inventory details, please contact USP product support, as it might be possible be re-implemented this functionality using the scheduled script engine built into USP NAS.