



# LDAP SCHEMA EXTENSION

The specifications and information in this document are subject to change without notice. Companies, names, and data used in examples herein are fictitious unless otherwise noted. This document may not be copied or distributed by any means, in whole or in part, for any reason, without the express written permission of RCDevs.

Copyright (c) 2010-2017 RCDevs SA. All rights reserved.

<http://www.rcdevs.com>

WebADM and OpenOTP are trademarks of RCDevs. All further trademarks are the property of their respective owners.

Limited Warranty

No guarantee is given for the correctness of the information contained in this document. Please send any comments or corrections to [info@rcdevs.com](mailto:info@rcdevs.com).

# LDAP Schema Extension

[Active Directory](#) [OpenLDAP](#) [Novell](#) [Schema](#)

## LDAP Schema Extension

### 1. Content of the Schema Extension

The schema extension is very minimal. It is composed of three object classes (*webadmAccount*, *webadmGroup* and *webadmConfig*) and three attributes (*webadmSettings*, *webadmData* and *webadmType*).

Each attribute contains a registered object identifier. *34617* corresponds to the registered number for RCDevs at [IANA](#).

### 2. Automatic Schema Extension

This option is preferred and is very easy. It works with most of LDAP servers.

#### 2.1 Active Directory Prerequisite

The first domain controller defined in `/opt/webadm/conf/servers.xml` should be a schema master.

We check which domain controller is the schema master with `Get-ADForest` in PowerShell:

```
PS C:\Users\administrator> (Get-ADForest).SchemaMaster
vagrant-2012-r2.test.local
```

The WebADM admin should be a schema admin, we can add it temporarily in the *schema admins* group in the AD.

We check that we are a member of the schema admins group with `Get-ADGroupMember`:

```
PS C:\Users\administrator> Get-ADGroupMember "schema admins"

distinguishedName : CN=Administrator,CN=Users,DC=test,DC=local
name              : Administrator
objectClass       : user
objectGUID        : 51be422c-e4cb-4463-a60f-fd9c4c0b63a3
SamAccountName    : Administrator
SID               : S-1-5-21-3541430928-2051711210-1391384369-500
```

#### 2.2 Schema Extension

We log in to WebADM:

We click on `Setup LDAP schema` :

We click on `Extend Schema` :

That's it, the schema is extended:

### 3. Manual Schema Extension with Active Directory

This method is not recommended but, in some rare cases, it is not possible to extend the schema of Active Directory through WebADM for internal security restrictions.

Some modifications in the schema cannot be undone, so you need to understand well how the schema works. Errors are not permitted in this procedure.

For the schema extension, we need to connect to the schema master domain controller with a schema administrator.

We check which domain controller is the schema master with `Get-ADForest` in PowerShell:

```
PS C:\Users\administrator> (Get-ADForest).SchemaMaster
vagrant-2012-r2.test.local
```

We check that we are a member of the *schema admins* group with `Get-ADGroupMember` :

```
PS C:\Users\administrator> Get-ADGroupMember "schema admins"

distinguishedName : CN=Administrator,CN=Users,DC=test,DC=local
name              : Administrator
objectClass       : user
objectGUID        : 51be422c-e4cb-4463-a60f-fd9c4c0b63a3
SamAccountName    : Administrator
SID               : S-1-5-21-3541430928-2051711210-1391384369-500
```

We search for the schema naming context:

```
PS C:\Users\administrator> (Get-ADRootDSE).schemaNamingContext
CN=Schema,CN=Configuration,DC=test,DC=local
```

We create the `schema.ldif` file with the following content.

`CN=Schema,CN=Configuration,DC=test,DC=local` must be replaced everywhere with the right schema naming context:

```
dn: CN=webadmSettings,CN=Schema,CN=Configuration,DC=internal,DC=theycyberhawk,dc=com
changetype: add
attributeID: 1.3.6.1.4.1.34617.2.3.1
attributeSyntax: 2.5.5.12
oMSyntax: 64
cn: webadmSettings
isSingleValued: TRUE
objectClass: attributeSchema
searchFlags: 0
```

```
dn: CN=webadmData,CN=Schema,CN=Configuration,DC=internal,DC=theycyberhawk,dc=com
changetype: add
attributeID: 1.3.6.1.4.1.34617.2.3.2
attributeSyntax: 2.5.5.12
oMSyntax: 64
cn: webadmData
isSingleValued: TRUE
objectClass: attributeSchema
searchFlags: 0
```

```
dn: CN=webadmType,CN=Schema,CN=Configuration,DC=internal,DC=theycyberhawk,dc=com
changetype: add
attributeID: 1.3.6.1.4.1.34617.2.3.3
attributeSyntax: 2.5.5.12
oMSyntax: 64
cn: webadmType
isSingleValued: TRUE
objectClass: attributeSchema
searchFlags: 0
```

```
dn: CN=webadmVoice,CN=Schema,CN=Configuration,DC=internal,DC=theycyberhawk,dc=com
changetype: add
attributeID: 1.3.6.1.4.1.34617.2.3.4
attributeSyntax: 2.5.5.10
oMSyntax: 4
cn: webadmVoice
isSingleValued: TRUE
objectClass: attributeSchema
searchFlags: 0
```

```
dn:
```

dn: -

changetype: modify  
add: schemaUpdateNow  
schemaUpdateNow: 1

dn: CN=webadmAccount,CN=Schema,CN=Configuration,DC=internal,DC=theycyberhawk,dc=com  
changetype: add  
cn: webadmAccount  
governsID: 1.3.6.1.4.1.34617.2.4.1  
mustContain: cn  
mustContain: sAMAccountName  
mayContain: webadmSettings  
mayContain: webadmData  
mayContain: webadmVoice  
mayContain: preferredLanguage  
mayContain: mobile  
mayContain: mail  
mayContain: description  
objectClass: classSchema  
objectClassCategory: 3  
subclassOf: top  
possSuperiors: container  
possSuperiors: domain  
possSuperiors: builtinDomain  
possSuperiors: domainDNS  
possSuperiors: organization  
possSuperiors: organizationalUnit

dn: CN=webadmConfig,CN=Schema,CN=Configuration,DC=internal,DC=theycyberhawk,dc=com  
changetype: add  
cn: webadmConfig  
governsID: 1.3.6.1.4.1.34617.2.4.2  
mustContain: cn  
mustContain: webadmType  
mayContain: webadmSettings  
mayContain: description  
objectClass: classSchema  
objectClassCategory: 1  
subclassOf: top  
possSuperiors: container  
possSuperiors: domain  
possSuperiors: builtinDomain  
possSuperiors: domainDNS  
possSuperiors: organization  
possSuperiors: organizationalUnit

dn: CN=webadmGroup,CN=Schema,CN=Configuration,DC=internal,DC=theycyberhawk,dc=com  
changetype: add  
cn: webadmGroup  
governsID: 1.3.6.1.4.1.34617.2.4.3  
mustContain: cn  
mayContain: webadmSettings  
mayContain: description

```
objectClass: classSchema
objectClassCategory: 3
subClassOf: top
possSuperiors: container
possSuperiors: domain
possSuperiors: builtinDomain
possSuperiors: domainDNS
possSuperiors: organization
possSuperiors: organizationalUnit
```

```
dn: -
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
```

```
dn: CN=User,CN=Schema,CN=Configuration,DC=internal,DC=thecyberhawk,dc=com
changetype: modify
add: auxiliaryClass
auxiliaryClass: webadmAccount
```

```
dn: CN=Group,CN=Schema,CN=Configuration,DC=internal,DC=thecyberhawk,dc=com
changetype: modify
add: auxiliaryClass
auxiliaryClass: webadmGroup
```

```
dn: -
changetype: modify
add: schemaUpdateNow
schemaUpdateNow: 1
```

Now we extend the schema. The `schema.ldif` file must be correct, we cannot undo this operation:

```
PS C:\Users\administrator> ldifde -i -f schema.ldif
Connecting to "vagrant-2012-r2.test.local"
Logging in as current user using SSPI
Importing directory from file "schema.ldif"
Loading entries.....
11 entries modified successfully.
```

That's it, the schema is extended.

*This manual was prepared with great care. However, RCDevs S.A. and the author cannot assume any legal or other liability for possible errors and their consequences. No responsibility is taken for the details contained in this manual. Subject to alternation without notice. RCDevs S.A. does not enter into any responsibility in this respect. The hardware and software described in this manual is provided on the basis of a license agreement. This manual is protected by copyright law. RCDevs S.A. reserves all rights, especially for translation into foreign languages. No part of this manual may be reproduced in any way (photocopies, microfilm or other methods) or transformed into machine-readable language without the prior written permission of RCDevs S.A. The latter especially applies for data processing systems. RCDevs S.A. also reserves all communication rights (lectures, radio and television). The hardware and software names mentioned in this manual are most often the registered trademarks of the respective manufacturers and as such are subject to the statutory regulations. Product and brand names are the property of RCDevs S.A. © 2021 RCDevs SA, All Rights Reserved*

