



APPFIELDUC - ADMIN GUIDE

Admin Guide

Version 3.7.4

© Netfarmers GmbH

INHALT

1	NFAppfieldManager & NFAppfieldUC	4
1.1	Requirements	4
1.1.1	Hardware	4
1.1.2	Cisco Unified Communication Manager	4
1.1.3	Cisco IP Phones / Cisco Jabber	5
1.1.4	Port Usage	5
1.1.5	Browser	6
1.2	Command Line Access	6
1.2.1	Network Configuration	7
1.2.2	DNS & NTP Configuration	7
1.2.3	Services and Restart Options	8
1.2.4	Other Options	8
1.3	Web Frontend	9
1.3.1	Services	9
1.3.2	Configuration	10
1.3.3	License	14
1.3.4	Certificates	16
1.3.5	Backup and Recovery	24
1.3.6	System	25
1.3.7	Troubleshooting	27
1.3.8	User	28
2	NFChefSek	29
2.1	CUCM Configuration	31
2.1.1	BLF Feature Configuration	31
2.1.2	External Call Control Profile	35
2.1.3	XML Service	36
2.1.4	MultiSek Feature	37

2.1.5	Device Configuration	38
2.2	NFChefSek Configuration.....	42
2.2.1	Base Configuration	42
2.2.2	Secretary Configuration	45
3	NFBusyTrigger	47
3.1	CUCM Configuration	47
3.1.1	XML Service	47
3.2	NFBusyTrigger Configuration.....	48
4	NFCallForwarder	50
4.1	CUCM Configuration	50
4.1.1	XML Service	50
4.2	NFCallForwarder Configuration	51
5	NFCompanyDirectory	53
5.1	CUCM Configuration	53
5.1.1	XML Service	53
5.2	NFCompanyDirectory Configuration	55
6	NFOffice-UC.....	57
6.1	CUCM Configuration	57
6.1.1	Custom Jabber Tab	57
6.1.2	Mobile Remote Access (MRA) Support	58
6.1.3	Mobile Device Integration	59
6.2	NFOffice UC Configuration	60
6.3	SAML SSO Configuration.....	61
6.3.1	Microsoft AD FS Configuration	61
6.3.2	Appfield Configuration	64
6.3.3	Microsoft AD FS Troubleshooting	65
7	NFCallList.....	66
7.1	CUCM Configuration	67
7.1.1	XML Service	67
7.1.2	Custom Jabber Tab	67

7.1.3	Custom WebEx Tab	68
7.1.4	CDR Enablement.....	69
7.1.5	CDR Management Configuration	70
7.1.6	JTAPI User Access Rights	70
7.2	NFCallList Configuration	71
7.3	SAML SSO Configuration.....	73
7.3.1	Microsoft AD FS Configuration	73
7.3.2	Appfield Configuration	77
7.3.3	Microsoft AD FS Troubleshooting	78
8	NFContacts	79
8.1	CUCM Configuration	80
8.1.1	External Call Control Profile	80
8.1.2	Update Translation Pattern.....	81
8.2	NFContacts Configuration.....	82
8.2.1	Sample CSV File	84
9	OS Upgrades.....	85
9.1	Fresh Install.....	85
9.1.1	Preparation.....	85
9.1.2	Setup the new server	85
9.1.3	In Maintenance Window	86
9.2	OS Upgrade via CLI.....	86
9.2.1	Preparation.....	87
9.2.2	Upgrade to inactive partition	87
9.2.3	Switch partition	88

1 NFAPPFIELDMANAGER & NFAPPFIELDUC

The Appfield UC appliance is a unified solution for easy and quick administration of the NF Apps. All NF Apps are seamlessly integrated into the appliance, and you can use the web interface to administrate, configure and maintain the apps.

1.1 REQUIREMENTS

1.1.1 HARDWARE

For initial implementation you'll receive a virtual machine template that is preinstalled with operating system and NFAppfieldManager App.

The VM template (starting Version 2.0 or greater) has the following hardware requirements as listed below:

- 16 GB Ram
- Dual Core CPU w. min. 2 Ghz (4x vCPU)
- 160 GB HDD

The minimum VMWare ESXi version is 6.5

1.1.2 CISCO UNIFIED COMMUNICATION MANAGER

We support the following CUCM versions:

- Cisco Unified Communications Manager Version 11.5 (SU3 and later*)
- Cisco Unified Communications Manager Version 12.5
- Cisco Unified Communications Manager Version 14.0

Note:

NFAppfield 2.0 supports TLS 1.2 only- Therefore CUCM 11.5 Minimum is SU3 and later.

1.1.3 CISCO IP PHONES / CISCO JABBER

We support the following Cisco IP Phones / Jabber with the specified versions/protocols:

Device Series	Protocol	PhoneLoad	Remarks
Cisco 7900 Series	SIP / SCCP	SCCP41.9-4-2-1S * ¹ SCCP42.9-4-2SR1 * ¹ SCCPP45.9-4-2-1S * ¹ SIP41.9-4-2-1S * ¹ SIP42.9-4-2SR1 * ¹ SIP45.9-4-2-1S * ¹	BLF Feature in SCCP Load not supported for NFChefSek Wireless and Conference Phones are not supported.
Cisco 7800 Series	SIP	sip78xx.11-5-1-18 * ²	
Cisco 8800 Series	SIP	sip88xx.12-7-1-0001-393* ² sip8845_65.12-7-1-0001-393* ²	Wireless and Conference Phones are not supported.
Cisco 9900 Series	SIP	sip9951.9-4-2SR2-2* ² sip9971.9-4-2SR2-2 * ²	
Cisco Jabber (CSF)	HTTP/HTTPS	12.8.1 Build 302494 * ²	IE Version 11 or later for MS Windows OS

Table 1: Supported Cisco IP Phones

*¹ = PhoneLoad must match this version. **Latest phoneload has currently a bug with XML services.**

*² = Tested with specified version, other versions may work but haven't been tested.

Note:

NFAppfield 2.0 supports TLS 1.2 only, there's no interoperability for earlier TLS versions; make sure that the phones do support this standard. Older phone models might not be able to support this!

Due to phone load updates, there might arise issues with XML services and the embedded browser engine. In case of problems, please contact us via E-Mail support@netfarmers.net.

1.1.4 PORT USAGE

The following table contains all ports of the communications.

Source	Destination	Port	Remarks
IP Phones / Jabber	Appfield-UC	443/TCP 8443/TCP	XML Services in https Mode 8443 is optional.
Administrators	Appfield UC	80/TCP	Appfield UC Administration Redirect to HTTPS

Administrators	Appfield UC	443/TCP	Appfield UC Administration
Administrators	Appfield UC	22/TCP	Appfield UC Administration
Appfield UC	CUCMs	8443/TCP	AXL Request/Response
CUCMs	Appfield UC	443/TCP 8443/TCP	External Call Control Profile (NFChefSek App). 8443 is optional.
Appfield UC	CUCMs	5060/TCP	SIP BLF Subscribe/Notify (NFChefSek App)
CUCMs	Appfield UC	5060/TCP	SIP BLF Subscribe/Notify (NFChefSek App)
CUCM Publisher	Appfield UC	22/TCP	CDR Collection (NFCallList App)
Appfield UC	LDAP Server	389/TCP	LDAP Directory Queries (NFCompanyDirectory App) or any other LDAP Port (configurable)
Appfield UC	Mail Server	25/TCP	eMail Notifications (Alarms & NFApp Notifications)

Table 2: List of TCP ports

The “Disable http Access” option has been decommissioned for security reasons and is no more available for NF Apps. Please ensure that certificates and TLS communications is configured properly.

1.1.5 BROWSER

In general, we try to make sure that latest Browser versions (Chrome, Firefox, Microsoft Edge) are compatible.

We do not recommend not to use old Internet Explorer versions, as problems have been identified with file and license uploads.

1.2 COMMAND LINE ACCESS

Appfield UC provides a Command Line Interface (CLI) for basic configuration settings. We recommend to perform initial configuration of VM using the CLI to provide IP access in customer network.

When IP configuration is complete you can also use SSH (e.g. putty) to connect to Appfield UC.

Default credentials:

Username: admin

Password: admin

Regardless of using CLI or SSH, you'll see after successful login the main menu that provides all basic configuration options to make Appfield UC available in the customer network.

```
*****
Main Menu:
  1) Network Settings
  2) DNS & NTP Settings
  3) Change Passwords
  4) Services and Restart Options
  5) SNMP Configuration
  6) Wireshark Tracing
  7) Full Trace Collection Tool
  8) OS Upgrade Menu

  0) Exit
*****
Select Option: █
```

Figure 1: CLI – main menu

1.2.1 NETWORK CONFIGURATION

Using main menu step 1) you are able to set static IP configuration. As shown below you'll see the current configuration settings and are able to change them using 1). The dialog will guide you through the IP configuration dialog.

You need to specify IP-Address, Subnet Mask and the default Gateway. When completed the wizard will reset the network interface automatically. In case you are connect using IP (instead of console), you will be disconnected from SSH session.

```
*****
Menu: Network Settings
      IP Address:    10.1.1.19
      Subnet Mask:   255.255.255.0
      default Gateway 10.1.1.254

  1) Change Network Settings
  0) Exit

Note: Changing settings will cause a
      network interruption.
*****
Select Option: █
```

Figure 2: CLI – network configuration

1.2.2 DNS & NTP CONFIGURATION

Using main menu step 2) you are able to set DNS and NTP settings. As shown below you'll see the current configuration settings and are able to change according to the number shown in on the screen.

The parameter “DNS Suffix” will be used to form the Full Qualified Domain Name (FQDN).

When changing any of the parameters the network interface will be reset, which may lead to an interruption.

```
*****
Menu: DNS & NTP Settings
      Hostname      appfield1
      DNS Suffix     lab.netfarmers.net
      DNS Servers    10.1.1.40,
      NTP Servers    10.1.1.40,

1) Change Hostname
2) Change DNS Suffix
3) Change DNS Servers
4) Change NTP Servers

0) Exit

Note: Changing settings will cause a
      network interruption.

*****
Select Option: █
```

Figure 3: CLI - DNS & NTP Configuration

1.2.3 SERVICES AND RESTART OPTIONS

Using main menu step 4) you are able to Restart the Tomcat service, Reboot the complete operating system or shutdown the Appfield UC appliance for maintenance.

Please make sure that you will not be asked to confirm, the requested action will be performed directly.

We highly recommend to use the shutdown option listed here for maintenance jobs and **do not stop** the VM in VMware ESXi interface.

```
*****
Menu: Services and Restart Options
1) Restart Tomcat Service
2) Restart System
3) Shutdown System

0) Exit
*****
Select Option: █
```

Figure 4: CLI – Services and Restart Options

1.2.4 OTHER OPTIONS

The CLI provides the following other options for configuration and troubleshooting:_

- Change Passwords for cdradmin & appupp user accounts (Option 3)
- Configure SNMP (Option 5)
- Start & Stop a PCAP Tracing aka Wireshark (Option 6)
- In case of issues you can collect traces (Option 7)

- OS Upgrades (Option 8)

1.3 WEB FRONTEND

Once you have initially configured the network setting using the CLI, you are able to configure Appfield UC using the Web Frontend. Please use the URL...

Error! Hyperlink reference not valid.

...to access the appliance. You will automatically redirected to the sign in area.

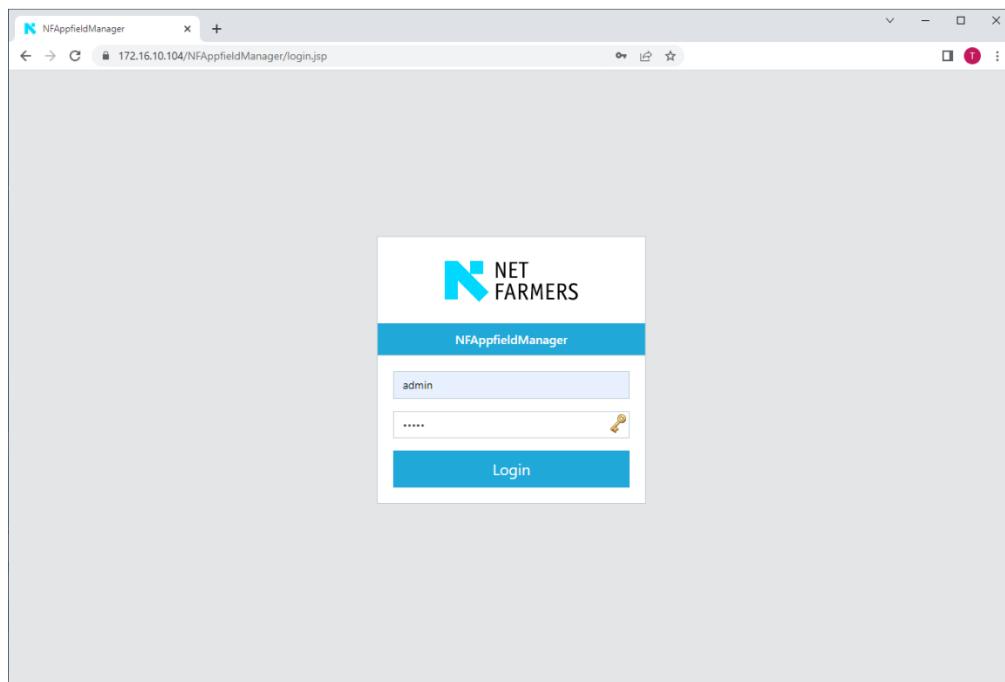


Figure 5: Appfield UC - Login

The default credentials are specified below and should be changed during initial configuration. Please note that the Web Frontend and CLI credentials are identical.

Username: admin

Password: admin

1.3.1 SERVICES

With the menu „Services“ you'll see all installed NF Apps and you see further information's, as the version number.

By default, our VMWare image will provide you all NF Apps which are just limited by the installed license. You see all NF Apps installed listed in this section. Please note that NFAppfieldManager is a core service

and you are not able to undeploy this service. However you are of course able to upload a new version of NFAppfieldManager.

Installed Services		
Service	Version	Remove
NFAppfieldManager	20190102-162921.8d535e9	
NFAppfieldUC	20190102-143244.16ed586	
NFAttendant	20181127-084124.30589b1	
NFBusyTrigger	3.4.269	
NFCDRReports	NOT RUNNING	
NFCallList	20190104-153934.928aea0	
NFCallforwarder	3.4.252	
NFChefSek	20190102-152943.8673a2e	
NFCompanyDirectory	3.2.158	
NFContacts	20190102-143418.c17d56c	
NFOfficeUC	20190104-122747.05ca46b	

Upload Service

Choose file

Upload

Figure 6: Web Frontend – Services

By using the Upload function, you can upgrade (or downgrade) to a newer software version of an NF App. For updates you'll receive a file with the filename syntax "<NF App Name>.war". This .war file must be uploaded in this section. You should ensure that the filename is equal to the existing Servicename (e.g. NFCallforwarder > NFCallforwarder.war). When pressing upload, the new service will be installed and initialized. The configuration data will remain in the database for updates and will be used in the new NF App software version.

Upload Service

Choose file

Upload

Figure 7: Web Frontend – Upload Services

Please note that upload and installation procedure may take a while, so do not refresh or change the browser window. Upload procedure shouldn't take more than 30 minutes, otherwise a failure may have occurred.

To remove NF App, use the "Remove" section. However the configuration data of this app will remain in database, so in case you re-deploy the NF App all configuration data will show up.

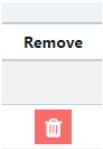


Figure 8: Services – Remove Service

Using the button „Status Page“, you'll get a new windows and are able to verify that the NF App is running and licensing is okay.

All NF Apps have individual configuration parameters to setup the service to your requirements. This section will show you the configuration settings of the main NFAppfieldManager and NFAppfieldUC service.

This NFAppfieldManager provides High Availability functions, web administration interface, mail notification and firewall / security configurations.

The screenshot displays the 'Settings' page of the NFAppfieldManager web frontend. The page is organized into three main sections: 'E-Mail Settings', 'Issue Mailer Settings', and 'Encryption Key'. Each section contains various configuration fields and checkboxes. The 'E-Mail Settings' section includes fields for SMTP Server, Username, Password, SSL Enabled, and Sender E-Mail. The 'Issue Mailer Settings' section includes checkboxes for Send Issue E-Mails, Include Service Issues, Include Expires Certificates, and Include License Issues, along with fields for Issue E-Mail Reciver, Issue E-Mail Subject, and Certificate Warning Before Days. The 'Encryption Key' section shows a text field with the value 'VzEj93AcOG0='. A 'Save Settings' button is located at the bottom left of the configuration area.

Section	Field/Option	Value/Status
E-Mail Settings	SMTP Server	IP of the smtp server
	Username	If authentication is needed than specifiy the username.
	Password	If authentication is needed than specifiy the password.
	SSL Enabled	<input type="checkbox"/>
	Sender E-Mail	Sender email address that is used.
Issue Mailer Settings	Send Issue E-Mails	<input type="checkbox"/>
	Issue E-Mail Reciver	E-Mail address of the reciver of issue reports.
	Issue E-Mail Subject	Subject
	Include Service Issues	<input checked="" type="checkbox"/>
	Include Expires Certificates	<input checked="" type="checkbox"/>
	Certificate Warning Before Days	30
Encryption Key	Encryption Key	VzEj93AcOG0=

Save Settings

Figure 9: Web Frontend – Configuration NFAppfieldManager

This NFAppfieldUC service will hold all configuration settings to connect with Cisco Unified Communications Manager Cluster. It will also provide High Availability functions and check for availability of configured CUCM nodes.

Settings

CUCM Availability Settings: ⓘ

CUCM Primary Node: ⓘ 172.16.10.101

CUCM Secondary Node: ⓘ 172.16.10.102

Availability Check Enabled: ⓘ ☒

AXL Response Timeout (ms): ⓘ 2500

SwitchBack Timer (m): ⓘ 5

Cronjob Settings: ⓘ

Login Validation Job: ⓘ ☒

Auth Validation Hour (h): ⓘ 4

Save Settings

Service » NFAppfieldUC

Configuration Help Application Log

Admin Tools

Run CUCM Cache Job (DNs, E-Mails) Refresh CUCM Cache Now

Run CUCM Auth Validation Job (Jabber credentials) Auth Validation Now

CUCM Settings

AXL Connection Status: ✓

Active CUCM: ⓘ 172.16.10.102

Username: ⓘ Administrator

Password: ⓘ *****

Save Settings

Figure 10: Web Frontend – Configuration NFAppfieldUC

The configuration parameters will be explained below in following table or in the web interface by click on the information icon (ⓘ).

Parameter	Description
CUCM Settings & CUCM Failover	
CUCM Primary Node	Enter the IP of the CUCM node that should be used primarily for AXL and UDS requests. Availability will be checked every 10 seconds automatically, 3 failed checks will result in a switch to the secondary node.
CUCM Secondary Node	Enter the IP of the CUCM node that should be used as backup for AXL and UDS requests. Availability will be checked every 10 seconds automatically, 3 failed checks will result in a switch to the secondary node. SwitchBack to primary node will be done according to SwitchBack Timer parameter.
AXL Response Timeout	Enter the amount of time (in milliseconds), that Appfield Manager will wait for an AXL response message to receive, when exceeded Appfield Manager will switch to secondary node.

SwitchBack Timer	Enter the amount of time (in Minutes), that Appfield Manager will wait after primary node has detected being available.
Backup Settings	
Enable Backup Scheduling	Set this parameter to enabled creation to sFTP Backup server.
sFTP Server IP	Enter the IP of the sFTP Server. Port 22 is default and non-configurable.
Username	Enter the username with access rights to the sFTP Backup Server.
Password	Enter the password of the specified user.
Path	Enter the path used within sFTP Backup Server. Use "\" for root directory.
Frequency	Specify the interval used for backups, e.g. 1= daily, 7= weekly
Number of Backups stored on sFTP Server	Specify the number of backups stored on the sFTP Server. Older backups will be deleted by Appfield UC appliance.
Last successful backup	The value shown provides the information, when the last successful backup has been created.
Appliance Cluster Settings	
Cluster Auth	Key for the cluster authentication.
Cluster Name	Name for the cluster.
Cluster Failover	Failover Host.
Disable http Access (deprecated)	This option, when set to true, disables http (port 80) access to Appfield UC for the specified App. When set to true only https (port 443) is available. Make sure to trust the certificate in CUCMs OS configuration ("phone-trust" truststore) for IP-Phones. For Jabber clients verify that Appfield Manager certificate is trusted by client's OS truststore. When using LSCs make sure to import CAPF certificate chain into Appfield Mangers truststore.

Table 3: NFAppfieldManager configuration parameters

1.3.2.1 CUCM AXL USER

For many services is Appfield UC using AXL to configured CUCM Cluster, we therefore need a AXL User that has read/write permissions to CUCM Cluster. Add a new Application User in CUCM with the configuration settings below, it is important to provide the roles "Standard AXL API Access" and "Standard AXL API Users" to this Application User.

Application User Configuration

Save Delete Copy Add New

Status

Status: Ready

Application User Information

User ID* axladmin

Password

Confirm Password

Digest Credentials

Confirm Digest Credentials

BLF Presence Group* Standard Presence group

☐ Accept Presence Subscription

☐ Accept Out-of-dialog REFER

☐ Accept Unsolicited Notification

☐ Accept Replaces Header

Permissions Information

Groups axladmins [View Details](#)

Roles Standard AXL API Access
Standard AXL API Users [View Details](#)

Figure 11: CUCM – AXL User

1.3.3 LICENSE

In menu step „License“ you are able to upload or review your uploaded license files.

We may provide you two typed of licenses:

- **Time based or Trials:**
Those type of licenses will contain an END DATE shown, after expiration of license the services will stop to work.
- **Permanent:**
A permanent license does not have an END DATE specified and is valid for the specified major release software version.

Appliance Information	
Name	Value
Appliance IP	172.16.10.104
Appliance Mac	00-50-56-98-B6-A7

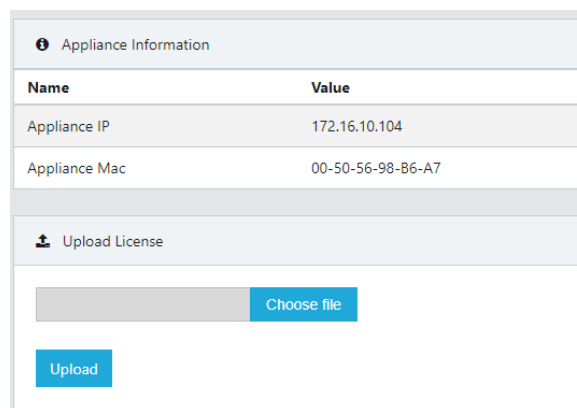
Figure 12: Web interface - License

The section appliance information will show you all required data that is needed to request a license file for your appliance. The data shown in appliance information is based on current configuration, so before requesting a license make sure that the data is correct.

To request a license mail to support@netfarmers.net with the following data:

- Applications
- Appliance IP
- Appliance MAC
- CUCM Hosts
- Appliance virtual IP*
- Alternate Backup Host IP*

* Only necessary if you want use clustering with two appliances instances



Appliance Information	
Name	Value
Appliance IP	172.16.10.104
Appliance Mac	00-50-56-98-B6-A7

Upload License

Figure 13: Web interface - License upload

When requested a license file you can upload the file in the “Upload License” section. After completion of upload process the license settings will show in the section “Active License”:

Active License	
Name	Value
APPLIANCE-ALTERNATE-HOST	172.16.10.105
APPLIANCE-HOST	172.16.10.104
APPLIANCE-MAC	00-50-56-98-B6-A7
APPLIANCE-PRIORITY	master
APPLIANCE-VIRTUAL-IP	172.16.10.106
APPLICATIONS	<ul style="list-style-type: none"> • NfChefSek • NfBusyTrigger • NfCallforwarder • NfOfficeUC • NfCompanyDirectory • NfContacts • NfCallList • NfAttendant • NfUCDataExport
COMPANY	lab.netfarmers.net
START-DATE	2018-01-01

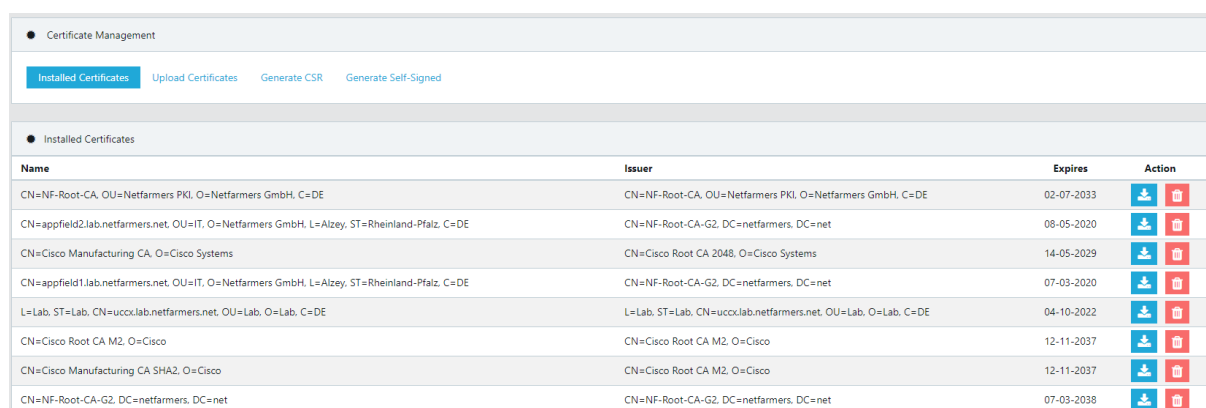
Figure 14: Web interface - Active License

Please note that validity of a license will be interval based count check of existing Endusers and Phones in the Cisco Unified Communications Manager.

1.3.4 CERTIFICATES

Appfield UC Appliance provides security implementations such as TLS by using certificates. By default, the appliance is in secure mode, which allows access to the Web Frontend using http, being redirected to https also access to XML Phone Services is only available using https.

In the Web Frontend you'll see the menu Certificates which provides you several options, to upload, remove and generate certificates.



The screenshot shows the 'Certificate Management' section of the Web Frontend. It includes tabs for 'Installed Certificates', 'Upload Certificates', 'Generate CSR', and 'Generate Self-Signed'. Below the tabs is a table titled 'Installed Certificates' with columns for Name, Issuer, Expires, and Action. The table lists several certificates, including those for Netfarmers PKI, Netfarmers GmbH, and Cisco Systems.

















Name	Issuer	Expires	Action
CN=NF-Root-CA, OU=Netfarmers PKI, O=Netfarmers GmbH, C=DE	CN=NF-Root-CA, OU=Netfarmers PKI, O=Netfarmers GmbH, C=DE	02-07-2033	 
CN=appfield2.lab.netfarmers.net, OU=IT, O=Netfarmers GmbH, L=Alzey, ST=Rheinland-Pfalz, C=DE	CN=NF-Root-CA-G2, DC=netfarmers, DC=net	08-05-2020	 
CN=Cisco Manufacturing CA, O=Cisco Systems	CN=Cisco Root CA 2048, O=Cisco Systems	14-05-2029	 
CN=appfield1.lab.netfarmers.net, OU=IT, O=Netfarmers GmbH, L=Alzey, ST=Rheinland-Pfalz, C=DE	CN=NF-Root-CA-G2, DC=netfarmers, DC=net	07-03-2020	 
L=Lab, ST=Lab, CN=uccolab.netfarmers.net, OU=Lab, O=Lab, C=DE	L=Lab, ST=Lab, CN=uccolab.netfarmers.net, OU=Lab, O=Lab, C=DE	04-10-2022	 
CN=Cisco Root CA M2, O=Cisco	CN=Cisco Root CA M2, O=Cisco	12-11-2037	 
CN=Cisco Manufacturing CA SHA2, O=Cisco	CN=Cisco Root CA M2, O=Cisco	12-11-2037	 
CN=NF-Root-CA-G2, DC=netfarmers, DC=net	CN=NF-Root-CA-G2, DC=netfarmers, DC=net	07-03-2038	 

Figure 15: Web Frontend - Certificates

Please refer to the next chapter and make yourself comfortable with the security concept implemented in Appfield UC to understand how certificate based security has been implemented.

1.3.4.1 SECURITY CONCEPT

The following section explains the security concept to make the platform secure. Typical XML service applications use only http with no sufficient authentication. This makes attackers very easy to manipulate the XML Service with manipulated http calls. Just imagine, in an unsecure environment, an attacker could activate the forwarding of a manager to any number. Therefore, it is important to secure these services. The following image shows all components of the appliance server.

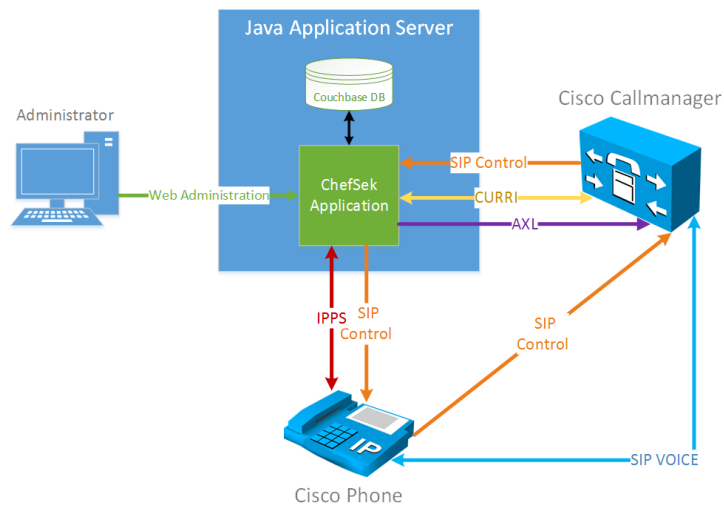


Figure 16: Appfield call flow with participants

Cisco Phones have by default a MIC Certificate (Manufacturer Installed Certificate) installed. In addition, administrators are able to add a CA signed certificate on the phone called LSC (Locally Signed Certificate) certificate. This certificate may be signed by a customer's Enterprise CA (via CAPF) or directly by CAPF service acting as a standalone Root CA.

When a Cisco Phone tries to access an XML Service using HTTPS, the appliance server requests a trusted certificate from the phone. The phone will use either the LCS or the MIC and present it to the Appfield UC appliance. The phone will prefer to present the LSC, in case it does not exist it will try to present the MIC.

By default, we have already imported the Cisco CA's that have been used to sign the MICs of Cisco IP Phones, which means that we trust a Cisco IP Phone using MICs. However, if you use LSCs on your IP Phones you have to make sure to upload the CA certificate from CAPF (capf.pem) and if used the Enterprise rootCA.

The figure below shows the communication flow of a https enabled XML service (e.g. CallForwarder):

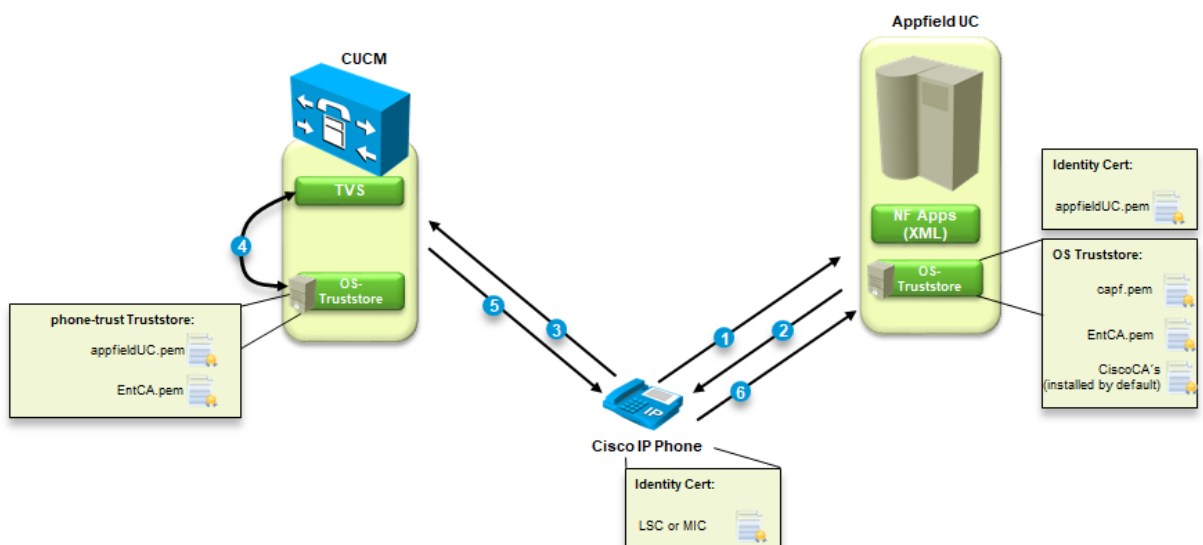


Figure 17: Appfield UC security concept

1. Cisco Phone will open the XML service using https.
2. Appfield UC will respond with a TLS handshake and present its identity certificate and will also request the phone to preset its own certificate.
3. From the IP Phone perspective, the presented certificate is unknown. The phone will ask the CUCM (TVS service) to authorize the presented certificate.
4. Based on the phone-trust truststore of the CUCM it will be able to verify that the appfieldUC.pem certificate is a trusted certificate.
5. TVS service will approve the certificate.
6. Cisco Phone will now complete the TLS handshake by presenting its own certificate, either MIC or (if exists) the LSC. When LSC is used, Appfield UC appliance needs to have CAPF.pem (and if used) EnterpriseCA certificate(s) imported.

1.3.4.2 SELF SIGNED APPFIELD CERTIFICATE

By default Appfield UC comes pre-installed with a self-signed certificates. This certificate may be regenerated using the “Generate Self-Signed” button.

Please note that Tomcat web service will be restarted and therefore the System will be unavailable for a short time.

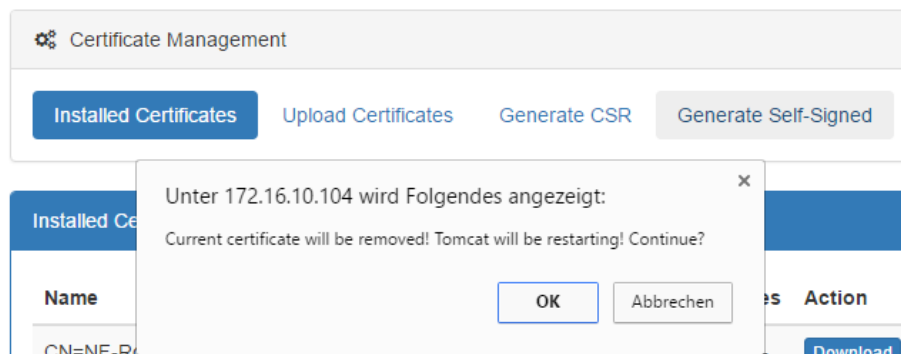


Figure 18: Web Frontend - Certificates

Generation of the self-signed certificate will be done based on the current network configuration (IP, Hostname, DNS Suffix). When changing network settings, you should make sure to regenerate the self-signed certificate.

1.3.4.3 CA SIGNED APPFIELD CERTIFICATE

Appfield UC appliance is able to create a CSR (Certificate Signed Request) to sign the Appfield UC certificate by an external CA (e.g. Enterprise CA).

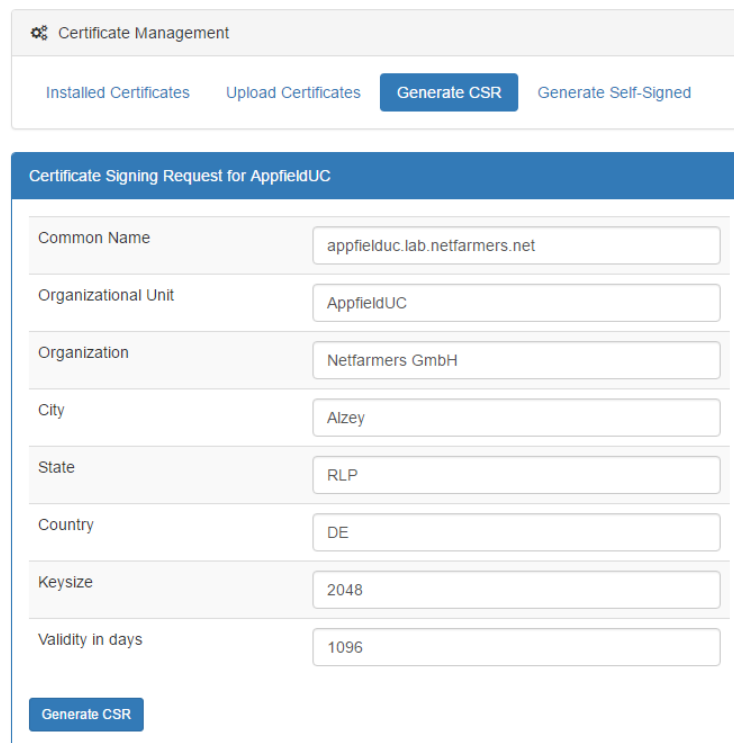
Please note that by default the CSR will create SANs (Subject Alternate Names) for:

- Hostname of Appfield UC
- FQDN of Appfield UC
- IP Address of Appfield UC

When HA is configured the following SANs will also be added:

- Cluster Name of Appfield UC
- Hostname of other Node
- IP of other Node
- Virtual IP of other Node

The figure below shows sample parameters for creating the CSR.



The screenshot shows the 'Certificate Management' web interface. At the top, there are tabs for 'Installed Certificates', 'Upload Certificates', 'Generate CSR' (which is active), and 'Generate Self-Signed'. Below the tabs is a form titled 'Certificate Signing Request for AppfieldUC'. The form contains the following fields and values:

Common Name	appfielduc.lab.netfarmers.net
Organizational Unit	AppfieldUC
Organization	Netfarmers GmbH
City	Alzey
State	RLP
Country	DE
Keysize	2048
Validity in days	1096

At the bottom of the form is a blue button labeled 'Generate CSR'.

Figure 19: Web Frontend - CSR

To sign the CSR by a Certificate Authority (CA) you need to make sure to:

- Allow to trust SANs from CSR, as Appfield will SANs when creating CSR:
 - <hostname of Appfield UC>
 - <IP of Appfield UC>
- Make sure to set enhanced key usage to:
 - Serverauthentication
 - Clientauthentication

The figure below shows an example of a Microsoft CA by applying a custom template:

Microsoft Active Directory Certificate Services – NF-Service-CA
Home

Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10 certificate request or PKCS #7 renewal request generated by an external source (such as a Web server) in the Saved Request box.

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

Certificate Template:

CiscoUC

Additional Attributes:

Attributes:

Submit >

Figure 20: Web Frontend – Sign CSR in CA

When CSR has been signed, you have to download the following files as base 64 encoded format (.pem):

- Identity certificate, which is the Appfield UC certificate signed by the CA.
- Intermediate (or Sub) CA certificate (if exists)
- Root CA certificate

Save all files as dedicated files and do not combine them!

Next step is to upload the CA certificates. Start with uploading the “Trusted (Root) Certificates” beginning with the Root CA certificate following (if exists) with the Intermediate CA certificate.

Certificate Management

Installed Certificates
Upload Certificates
Generate CSR
Generate Self-Signed

Upload Certificate (.pem)

☒ Trusted (Root) Certificates
☐ Signed Certificate

! Upload the following Manufacturer Installed Certificates from the CUCM certificate store:

- Cisco_Root_CA_M2
- Cisco_Manufacturing_CA
- Cisco_Manufacturing_CA_SHA2

NFrootCA.cer
Choose

Upload

Figure 21: Web Frontend – Upload trusted Certificates (root)

Certificate Management

Installed Certificates **Upload Certificates** Generate CSR Generate Self-Signed

Upload Certificate (.pem)

☒ Trusted (Root) Certificates ☐ Signed Certificate

! Upload the following Manufacturer Installed Certificates from the CUCM certificate store:

- Cisco_Root_CA_M2
- Cisco_Manufacturing_CA
- Cisco_Manufacturing_CA_SHA2

NFserviceCA.cer Choose

Upload

Figure 22: Web Frontend – Upload trusted Certificates (Intermediate)

When upload has been successful you will see them listed in “Installed Certificates” section of Appfield UC appliance.

Next step is to upload the identity certificate of Appfield UC appliance. Make sure to select “Signed Certificate” option and upload the file as shown. Please note that the filename is not relevant (here a .cer file is uploaded), however it is important to upload a certificate with Base64 encoding (also named “pem”).

Certificate Management

Installed Certificates **Upload Certificates** Generate CSR Generate Self-Signed

Upload Certificate (.pem)

☐ Trusted (Root) Certificates ☒ Signed Certificate

appfield.cer Choose

Upload

Figure 23: Web Frontend – Upload Identity certificate

1.3.4.4 TRUST RELATIONSHIPS

In order to have a trusted relation Cisco IP Phone and Appfield UC appliance, the CUCM must trust the Appfield UC appliance and vice versa. The following shows the configuration steps needed to set up a trust relationships for the different deployment scenarios:

Phones use MICs:

- Import Appfield UC certificate (and its certificate chain) into phone-trust and tvs-trust Truststore of CUCM.

- Import Appfield UC certificate (and its certificate chain) into callmanager-trust Truststore of CUCM, this is required for ECCP Profiles to work properly (ChefSek & NFCcontacts).

Phones use LCSs:

- Import Appfield UC certificate (and its certificate chain) into phone-trust and tvs-trust Truststore of CUCM.
- Import Appfield UC certificate (and its certificate chain) into callmanager-trust Truststore of CUCM, this is required for ECCP Profiles to work properly (ChefSek & NFCcontacts).
- Import capf.pem certificate (and its certificate chain) into Appfield UC as a “Trusted (Root) Certificate”.
- Import callmanager.pem certificate (and its certificate chain) for every CUCM Node into Appfield UC as a “Trusted (Root) Certificate”.

1.3.4.4.1 PHONES USING MIC

This configuration procedure is needed to set up a trust relationship of Cisco IP Phones with Appfield UC by using MIC certificates.

Step 1: Import Appfield UC certificate into CUCM cluster.

The following steps are necessary to import a certificate to the CUCM:

1. Browse to the OS Administration web website:
2. Open the menu item Security -> Certificate Management in the CUCM navigation.
3. Then click Upload Certificate / Certificate chain in the Toolbar.
4. A popup appears to upload a new certificate.
5. When you have Appfield UC signed by a CA, you have to upload the Root- and Intermediate CA certificates now, for using Appfield UC with self-signed certificate you can skip this step.
6. Select **phone-trust** as certificate purpose and select your certificate (.cer) file downloaded from Appfield UC appliance.

7. After pressing the “Upload” button, the certificate is imported and displayed in the certificate list.

8. Repeat this step and upload the same certificates into **callmanager-trust** truststore. You only need to upload to this truststore, when using External Call Control Profile function from NFApps (e.g. NFChefSek, NFCcontacts, ..)

Note: It can take a while until the phones receive the certificate. You receive the certificates immediately with a restart of the phones.

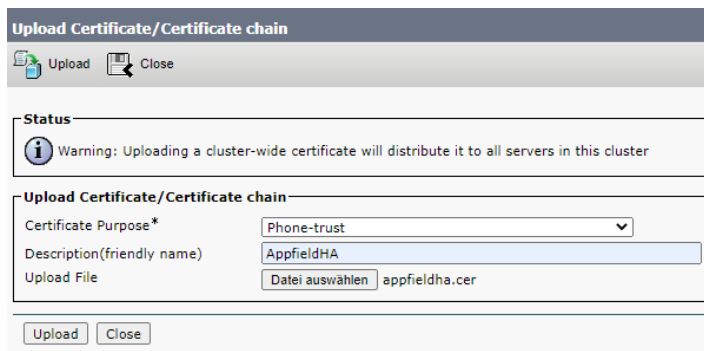
1.3.4.4.2 PHONES USING LSC

This configuration procedure is needed to set up a trust relationship of Cisco IP Phones with Appfield UC by using LSC certificates.

Step 1: Import Appfield UC certificate into CUCM cluster.

The following steps are necessary to import a certificate to the CUCM:

1. Browse to the OS Administration web website:
2. Open the menu item Security -> Certificate Management in the CUCM navigation.
3. Then click Upload Certificate / Certificate chain in the Toolbar.
4. A popup appears to upload a new certificate.
5. When you have Appfield UC signed by a CA, you have to upload the Root- and Intermediate CA certificates now, for using Appfield UC with self-signed certificate you can skip this step.
6. Select **phone-trust** as certificate purpose and select your certificate (.cer) file downloaded from Appfield UC appliance.



7. After pressing the "Upload" button, the certificate is imported and displayed in the certificate list.
8. Repeat this step and upload the same certificates into **callmanager-trust** truststore. You only need to upload to this truststore, when using External Call Control Profile function from NFApps (e.g. NFChefSek, NFCcontacts, ..)

Note: It can take a while until the phones receive the certificate. You receive the certificates immediately with a restart of the phones.

Step 2: Import capf.pem certificate (and its certificate chain) into Appfield UC as a “Trusted (Root) Certificate”.

The following steps are necessary to import a certificate to the Appfield UC appliance:

1. Browse to the Appfield UC appliance website.
2. Open the menu item Certificates / Upload Certificates.
3. Make sure to select “Trusted (Root) Certificate” option.
4. When you have CAPF service signed by a CA, you have to upload the Root- and Intermediate CA certificates now, for using CAPF with self-signed certificate you can skip this step.
5. Select CAPF.pem as certificate press the Upload button.

Certificate Management

Installed Certificates Upload Certificates Generate CSR Generate Self-Signed

Upload Certificate (.pem)

☒ Trusted (Root) Certificates ☐ Signed Certificate

Upload the following Manufacturer Installed Certificates from the CUCM certificate store:

- Cisco_Root_CA_M2
- Cisco_Manufacturing_CA
- Cisco_Manufacturing_CA_SHA2

CAPF.pem Choose

Upload

6. After pressing the “Upload” button, the certificate is imported and displayed in the certificate list in the “Installed Certificates” section.

Certificate Management

Installed Certificates Upload Certificates Generate CSR Generate Self-Signed

Installed Certificates

Name	Issuer	Expires	Action
CN=NF-Root-CA, OU=Netfarmers PKI, O=Netfarmers GmbH, C=DE	CN=NF-Root-CA, OU=Netfarmers PKI, O=Netfarmers GmbH, C=DE	02-07-2033	Download Remove
L=Lab, ST=Lab, CN=CAPF-5b5a8097, OU=Lab, O=Netfarmers GmbH, C=DE	L=Lab, ST=Lab, CN=CAPF-5b5a8097, OU=Lab, O=Netfarmers GmbH, C=DE	29-06-2021	Download Remove

1.3.5 BACKUP AND RECOVERY

The AppfieldManager provides an automatic backup feature. The setup can be done as shown in chapter 1.3.2. Only sFTP servers are supported for automated backup. It is possible to use the same sFTP as for the CUCM backup. In the additional parameters you can specify the interval frequency in days when the backups should be created. The backup file rotation defines how much backups should be stored before older backup files get deleted.

The Backup menu provides a manual backup which downloads a compressed snapshot of the current system setup with all settings. For restoring, just upload the backup file from the automatic or manual backup. After the restore the webserver restarts, which takes several minutes to restore the data.

Backup Settings

Enable Backup Scheduling: ☒

sFTP Server IP: 10.1.1.41

Username: cisco

Password: *****

Path: /AppField104/

Execution Hour: 23

Frequency: 7

Number of Backups stored on sFTP Server: 2

Last successful backup: 03.05.2018 - 23:01:55

Save Settings

Manual Backup

The backup file includes the following items: Application Settings, Application Data, License and Certificates.

Download

Restore Backup

After the recovery process restarts the tomcat service! This can take several minutes.

Choose file

Restore

Figure 24: Web Frontend - Backup

1.3.6 SYSTEM

The systems menu provides the core configuration settings to setup the appliance. Following section describe in detail the network, NTP and cluster configuration.

A control panel on top have common operation to restart the webserver or reboot/shutdown the virtual machine.

Appliance Control Panel

Restart Tomcat

Update System

Reboot System

Shutdown System

Restart Cluster Service

1.3.6.1 NETWORK CONFIGURATION

The network settings can be configured via the web interface or via the command line access (1.2.1).

***Note:** When saving the network settings, the appliance will reconfigure the network interface that will cause a short interruption to settings to apply.*

Network Configuration	
IP	172.16.10.104
Subnet	255.255.255.0
Default Gateway	172.16.10.2
Hostname	appfield1
DNS Suffix	lab.netfarmers.net
DNS Nameserver	10.1.1.40
<button>Save</button>	

1.3.6.2 NTP CONFIGURATION

In this section the time server configuration via NTP is done. Per default the Debian NTP servers are configured. A minimum of one server must be specified, the other servers can be empty!

NTP Configuration	
Server 1	10.1.1.40
Server 2	
Server 3	
<button>Save</button>	

1.3.6.3 CLUSTER CONFIGURATION

In the following section explain the setup of an appliance cluster. Failover and load balancing is important for a high availability environment. With the setup you can eliminate a single point of failure in case of a server crash and distribute the incoming load on two servers. In case one server fails, the other takes over.

The configuration can only be done on the master appliance that is defined in the license. The cluster name defines the hostname for the Virtual Cluster IP for example like "appfield-cluster.netfarmers.net".

Before start, make sure that both appliances have the correct network settings and finished with starting up! Otherwise it can corrupt the cluster setup! This process can take up the 5 minutes and do not close the browser window. During the process the certificates are regenerated that they contain all the hosts and ips of the cluster. After the setup both hosts are configured and ready to use.

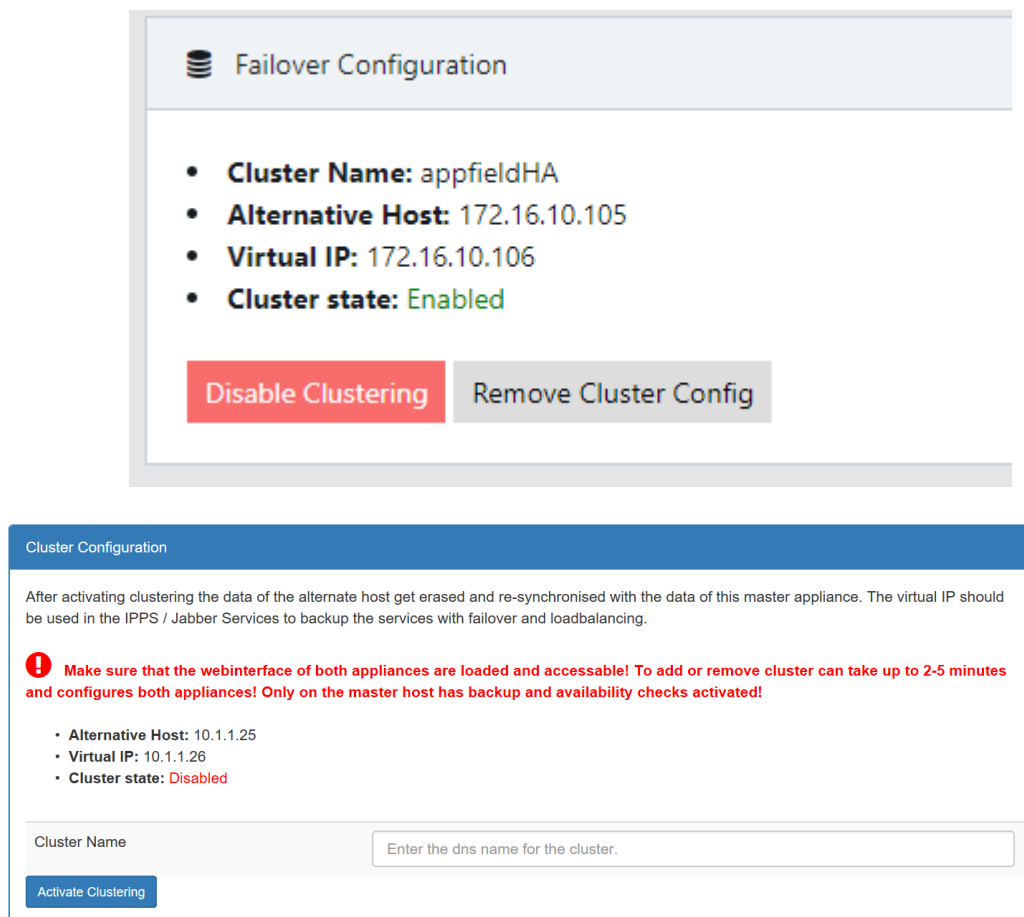


Figure 25: Web Frontend – Cluster configuration

1.3.7 TROUBLESHOOTING

Every services has a last tab that is called „Log“. Please note that log configuration is on a per service level available. You will see all logs shown by default in level ERROR. Depending on configured Log Level you may see in this pane a lot of log output. In case of any misconfiguration or application errors the log will show it in error level.

For troubleshooting you may need to set log level to Debug or Info, which will provide a full output of the specified application. **Logs of type Error will be highlighted in red.**

***Note:** Make sure to reset log level back to default „ERROR“ after completing logging.*

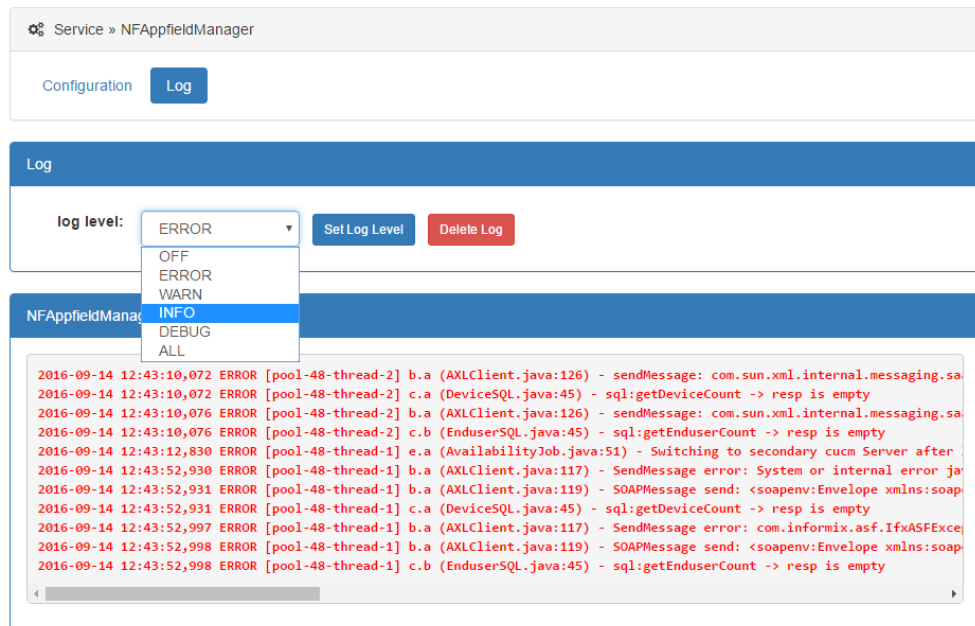


Figure 26: Web Frontend – Log troubleshooting

1.3.8 USER

You are able to make configuration changes of the logged in user in the upper right corner of the web interface Manual logout is available here and you are able to Change Password. Make sure that the password change applied to web application and OS user „admin“.

Note: After a change the restart of the tomcat is necessary to apply the change!

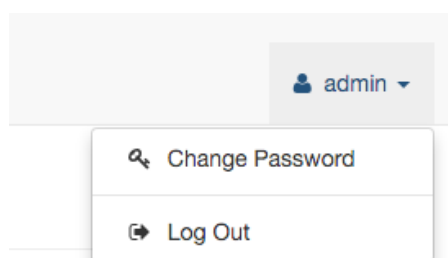
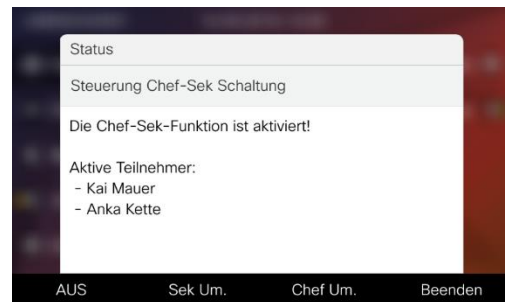


Figure 27: User Profil

Our NFChefSek App is a simple and intuitive Manager Assistant solution that provide the following features:

- Intuitive handling
- Flexible groups of Managers and Assistants
- Using BLFs for Status- and Control of ChefSek functions.
- Integration into Cisco Jabber (NFOfficeUC)
- Black- & Whitelists
- Flexible Proxy feature



By using BLFs for Status and Control of chefsec functions, the secretary or manager is able to quickly change settings with a single button.

The following functions may be controlled by a dedicated BLF:

- Diversion to Secretary (Umleitung Sekretariat), which means that all calls will be routed to configured secretaries.
- Diversion to Proxy (Vertretung) provides the ability to route calls to another colleague which is then allowed to transfer calls back to the manager.
- Pause (or Logout) is useful in environments with multiple secretaries.
- Manager-Forwarding, provides a forwarding to the configured destination instead of directly to the Manager's IP Phone. This forwarding is set in Appfield UC application logic and not a CUCM call forwarding, so it will not appear on the Managers phone display.



Figure 28: NFChefSek - BLFs

The figure above shows an Assistants phone (Mauer) with two managers Bo Densee and Andi Theke configured.

For every Manager we have a default BLF that provides information's about ringing, busy and available state and we can also use this BLF to pick up unanswered calls on the Managers DN.

We have also configured dedicated BLFs for Diversion to Proxy (Vertretung) and Diversion to Secretary (Umleitung Sekretariat).

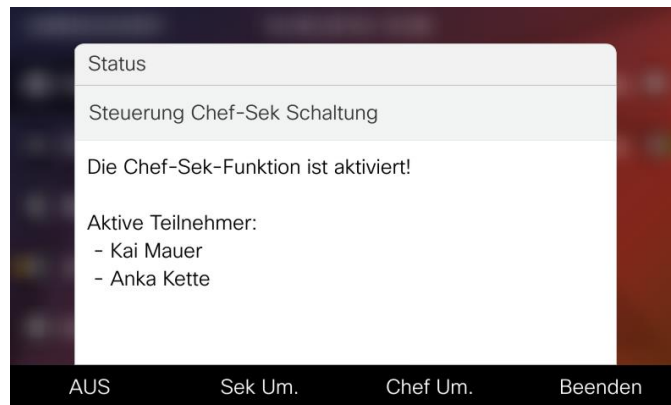


Figure 29: NFChiefSek - BLFs

Additionally, the secretary has a Service URL ("Einstellungen") that provides access to configuration settings like changing the DN for the Proxy. Please note that you can also enable or disable "Diversion to secretary" in case you do not want to spend a BLF for this feature.

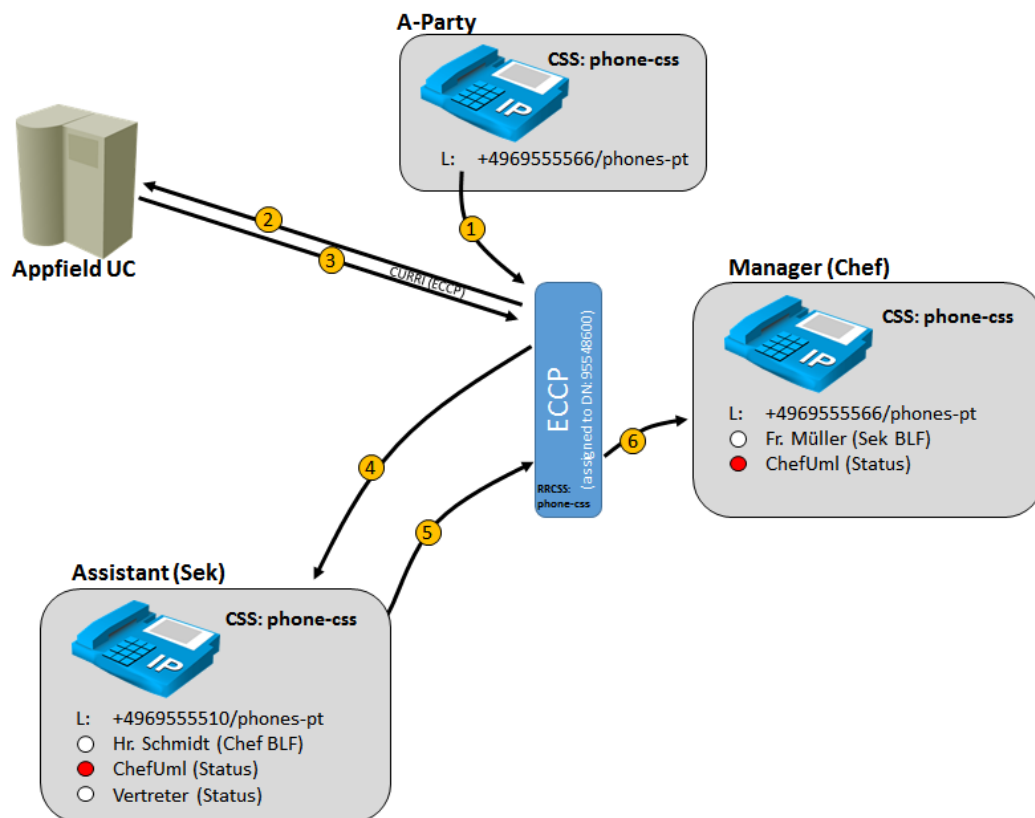


Figure 30: NFChiefSek – Routing Logic

The figure above gives an overview of the routing logic that is used in Appfield UC:

1. An internal or external user is calling the Manager.

2. Manager has been configured with External Call Control Profile (ECCP), which forwards the call request to Appfield UC.
3. As ChefUml BLF is enabled, calls should be diverted to Assistant, so Appfield UC will response with a diversion to the Assistants DN.
4. CUCM will divert the call based on assigned Rerouting CSS (configured in ECCP) to the Assistant, which can now answer the call.
5. Now Assistant will transfer to the Manager. ECCP will again route the request to Appfield UC (not shown in figure) and response to allow the call to the Manager.
6. As Appfield UC has permitted the call, the Managers DN will ring and transfer with A-Patry can be completed.

Additional features like Proxy, Manager-Forward or Black- and Whitelist with a similar logic.

2.1 CUCM CONFIGURATION

This chapter provides the configuration steps needed to implement NFChefSek on the CUCM.

The following list shows the required (and optional) configurations steps:

- BLF Feature Configuration
 - Create SIP Trunk Security Profile
 - Create SIP Profile
 - Create SIP Trunk
 - Create RouteList / RouteGroup (Optional)
 - Create SIP Route Pattern
- External Call Control Profile
- XML Service
- MultiSek Feature
- Device Configuration

2.1.1 BLF FEATURE CONFIGURATION

In order to control configuration settings of NFChefSek by using a BLF button, you'll need to perform the following configuration steps.

2.1.1.1 SIP TRUNK SECURITY PROFILE

In CUCM navigate to System / Security / SIP Trunk Security Profile and create a new profile with the settings as shown below:

SIP Trunk Security Profile Information	
Name*	Appfield-UC-Trunk
Description	
Device Security Mode	Non Secure
Incoming Transport Type*	TCP+UDP
Outgoing Transport Type	TCP
<input type="checkbox"/> Enable Digest Authentication	
Nonce Validity Time (mins)*	600
X.509 Subject Name	
Incoming Port*	5060
<input type="checkbox"/> Enable Application level authorization	
<input checked="" type="checkbox"/> Accept presence subscription	
<input checked="" type="checkbox"/> Accept out-of-dialog refer**	
<input checked="" type="checkbox"/> Accept unsolicited notification	
<input type="checkbox"/> Accept replaces header	
<input type="checkbox"/> Transmit security status	
<input type="checkbox"/> Allow charging header	
SIP V.150 Outbound SDP Offer Filtering*	Standardfilter verwenden

Save Delete Copy Reset Apply Config Add New

Figure 31: NfChefSek – SIP Trunk Security Profile

2.1.1.2 SIP PROFILE

In CUCM navigate to Device / Device Settings / SIP Profile and create a new profile with the settings as shown below:

SIP Profile Information

Name *	Appfield-UC - SIP Profile
Description	SIP Profile for Appfield-UC
Default MTP Telephony Event Payload Type *	101
Early Offer for G.Clear Calls *	Deaktiviert
User-Agent and Server header information *	Unified CM-Versionsinformationen als User-Agent-H
Version in User Agent and Server Header *	Haupt- und Nebenversion
Dial String Interpretation *	Alle Wahlzeichenfolgen immer als URI-Adressen be
Confidential Access Level Headers *	Deaktiviert

☐ Redirect by Application

☐ Disable Early Media on 180

☐ Outgoing T.38 INVITE include audio mline

☐ Offer valid IP and Send/Receive mode only for T.38 Fax Relay

☐ Use Fully Qualified Domain Name in SIP Requests

☐ Assured Services SIP conformance

☐ Enable External QoS **

SIP OPTIONS Ping

☒ Enable OPTIONS Ping to monitor destination status for Trunks with Service Type "None (Default)"

Ping Interval for In-service and Partially In-service Trunks (seconds) *	60
Ping Interval for Out-of-service Trunks (seconds) *	120
Ping Retry Timer (milliseconds) *	500
Ping Retry Count *	6

Figure 32: NFChefSek – SIP Profile

2.1.1.3 SIP TRUNK

In CUCM navigate to Device / SIP Trunk and create a new SIP Trunk with the settings as shown below:

Trunk Information

Trunk Type *	SIP Trunk
Device Protocol *	SIP
Trunk Service Type *	Keine (Standard)

Figure 33: NFChefSek – SIP Trunk 1

When pressing next you have to configure the trunk. Make sure to set the configuration's as highlighted below: **When configured please RESET Trunk to ensure it is in operational state.**

SIP Trunk Status

Service Status: Full Service

Duration: Time In Full Service: 0 day 0 hour 37 minutes

Device Information

Product: SIP Trunk

Device Protocol: SIP

Trunk Service Type: Keine (Standard)

Device Name*: Appfield-UC-Trunk

Description:

Device Pool*: Hamburg

Common Device Configuration: < None >

Call Classification*: Use System Default

Media Resource Group List: < None >

Location*: Hamburg

AAR Group: < None >

Tunneled Protocol*: Ohne

QSIG Variant*: Keine Änderungen

ASN.1 ROSE OID Encoding*: Keine Änderungen

Packet Capture Mode*: Keine

Packet Capture Duration: 0

☐ Media Termination Point Required
 ☒ Retry Video Call as Audio
 ☐ Path Replacement Support
 ☐ Transmit UTF-8 for Calling Party Name
 ☐ Transmit UTF-8 Names in QSIG APDU
 ☐ Unattended Port

SIP Information

Destination

☐ Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1 *	172.16.10.104		5060

MTP Preferred Originating Codec*: 711ulaw

BLF Presence Group*: Standard Presence group

SIP Trunk Security Profile*: Appfield-UC-Trunk

Rerouting Calling Search Space: < None >

Out-Of-Dialog Refer Calling Search Space: < None >

SUBSCRIBE Calling Search Space: CSS_Subscribe

SIP Profile*: Appfield-UC - SIP Profile

QSIG Signaling Method*:

Status: up

Status Reason:

Duration: Time Up: 0 day 0 hour 37 minutes

Figure 34: NfChefSek – SIP Trunk 2

As this trunk is not used for calls (just Presence Subscriptions) there's no need to assign an Inbound CSS or take care on Location, Region or Media Resource configuration settings.

2.1.1.4 ROUTE LIST / ROUTE GROUP (OPTIONAL)

You can use Route Group and Route Lists for the SIP Trunk created previously, however this configuration is not necessary.

To create a Route Group in CUCM navigate Call Routing / Route/Hunt / Route Group and create a new Route Group. Make sure to give it a descriptive name and assign the SIP Trunk created in the chapter before to the Route Group.

Next navigate to Call Routing / Route/Hunt / Route List and create a new Route List. Make sure to give it a descriptive name and assign the created Route Group to the Route List.

Make sure to reset the Route List and check that the Route List is registered with CUCM before proceeding.

2.1.1.5 SIP ROUTE PATTERN

In CUCM navigate to Call Routing / SIP Route Pattern and create a new SIP Route Pattern with the settings as shown below. When you have created a RouteList/RouteGroup assign the RouteList here.

SIP Route Pattern Configuration

Save Delete Copy Add New

Status

Status: Ready

Pattern Definition

Pattern Usage: Domänen-Routing

IPv4 Pattern*: appfield-uc.net

IPv6 Pattern:

Description:

Route Partition: phones

SIP Trunk/Route List*: Appfield-UC-Trunk (Edit)

☐ Block Pattern

Calling Party Transformations

☐ Use Calling Party's External Phone Mask

Calling Party Transformation Mask:

Prefix Digits (Outgoing Calls):

Calling Line ID Presentation*: Default

Calling Line Name Presentation*: Default

Connected Party Transformations

Connected Line ID Presentation*: Default

Connected Line Name Presentation*: Default

Save Delete Copy Add New

Figure 35: NFChefSek – SIP Route Pattern

2.1.2 EXTERNAL CALL CONTROL PROFILE

The External Call Control Profile (ECCP) is a core components for routing calls directly to the Manager or diverting the calls to an Assistant or Proxy (Vertreter).

In CUCM navigate to Call Routing / External Call Control Profile and create a new External Call Control Profile with the settings as shown below.

- Make sure to set the HTTP(s) URL to your Appfield UC Appliance IP:

Unsecure ECCP: http://<IP-of-AppfieldUC>:80/NFChefSek/CallRouting

Secure ECCP: https:// <IP-of-AppfieldUC>:443/NFChefSek/CallRouting

Be aware to keep the port information in the URL (e.g. :80) !!.

- Assign a Diversion Rerouting CSS that is able to:
 - Reach all DNs (e.g. Assistants, Proxys, etc.)

- **Optional:** Reach Forwarding Targets (e.g. Mobile Phone Numbers)

External Call Control Profile Configuration

Save Delete Copy Add New

Status
Status: Ready

External Call Control Information

Name* Appfield-ChefSek

Primary Web Service* http://172.16.10.104:80/NFChefSek/CallRouting

Secondary Web Service

☐ Enable Load Balancing

Routing Request Timer

Diversion Rerouting Calling Search Space CSS_Phones

Call Treatment on Failures* Anrufe zulassen

Save Delete Copy Add New

Figure 36: NFChefSek – External Call Control Profile

2.1.1.3 XML SERVICE

In CUCM navigate to Device / Device Settings / Phone Services and create a new phone service with the settings shown below:

- Make sure to set the HTTP(s) URL to your Appfield UC Appliance IP:

Unsecure: http://<IP-of-AppfieldUC>/NFChefSek/App?DeviceName=#DEVICENAME#

Secure: https:// <IP-of-AppfieldUC>/NFChefSek/App?DeviceName=#DEVICENAME#

IP Phone Services Configuration

Save Delete Update Subscriptions Add New

Status
Status: Ready

Service Information

Service Name* NFChefSek

Service Description Appfield-UC - ChefSek

Service URL* http://172.16.10.104/NFChefSek/App?DeviceName=#DEVICENAME#

Secure-Service URL

Service Category* XML-Dienst

Service Type* Standard-IP-Telefondienst

Service Vendor

Service Version

☒ Enable

Service Parameter Information

Parameters

New Parameter Edit Parameter Delete Parameter

Save Delete Update Subscriptions Add New

Figure 37: NFChefSek – XML Service

2.1.4 MULTISEK FEATURE

Our Multisek Feature is required when a group of Assistants should receive calls from a single Manager DN. By default an Assistant receives the call from a manager and can transfer the call back to the Manager. In a MultiSek environment, we have multiple active Assistants that receive the call from a Manager depending on the call distribution algorithm, e.g. Broadcast or Longest Idle.

For providing Multisek Feature we just use the logic of Hunt Pilot, Hunt List and Line Groups in CUCM.



Figure 38: NFChefSek – MultiSek Logik

This native CUCM functionality provides best routing of a single call to multiple Assistants. From a NFChefSek point of view, we divert the call to this Hunt Pilot in a MultiSek environment, while we divert the call directly to the Assistant in a non-Multisek environment.

The screenshot shows the 'Line Group Information' and 'Current Line Group Members' sections of the CUCM configuration interface.

Line Group Information

- Line Group Name*: ChefSek2.0_LG1
- RNA Reversion Timeout*: 10
- Distribution Algorithm*: Broadcast

Hunt Options

- No Answer*: Try next member; then, try next group in Hunt List
- ☐ Automatically Logout Hunt Member on No Answer
- Busy**: Try next member; then, try next group in Hunt List
- Not Available**: Try next member; then, try next group in Hunt List

Current Line Group Members

Reverse Order of Selected DN/Route Partitions

Selected DN/Route Partition: 95523008/PHONES-PT, 95548150/PHONES-PT

Removed DN/Route Partition:

Figure 39: NFChefSek - MultiSek - Line Group Configuration

When a Manager requires MultiSek Feature, you can just create a Line Group and add all Assistants into the Line Group created. Set the Distribution Algorithm that fits your needs and create Hunt List and Hunt Pilot with a DN reachable from Rerouting CSS of the External Call Control Profile.

2.1.5 DEVICE CONFIGURATION

To configure an IP Phone for NFChefSek, you have to perform some configurations on Manager and Assistant phone. The following table shows the configurations are required and optional:

Function	Manager	Assistant
Assign XML Service	Yes	Yes
Assign External Call Control Profile	Yes	No
Assign BLFs	Recommended, but not required	Recommended, but not required

Table 4: Chefsek - required device configuration

2.1.5.1 ASSIGN XML SERVICE

In CUCM navigate to Device / Phone. Now search for the Manager or the Assistant Phone. Select in the related Links section the “Subscribe/Unsubscribe Services” Option and subscribe the XML Services created before.

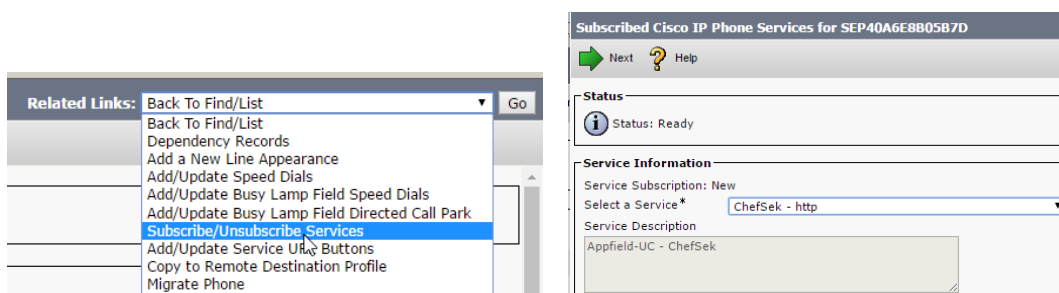


Figure 40: NFChefSek – Add Phone Service

You may rename the XML service to your needs on a per phone level (optional):



Figure 41: NFChefSek – XML Service Subscription

You can (optionally) give direct access to this XML service by using a Service URL button in the phone button template configuration. Please refer to the figure below for a sample configuration:

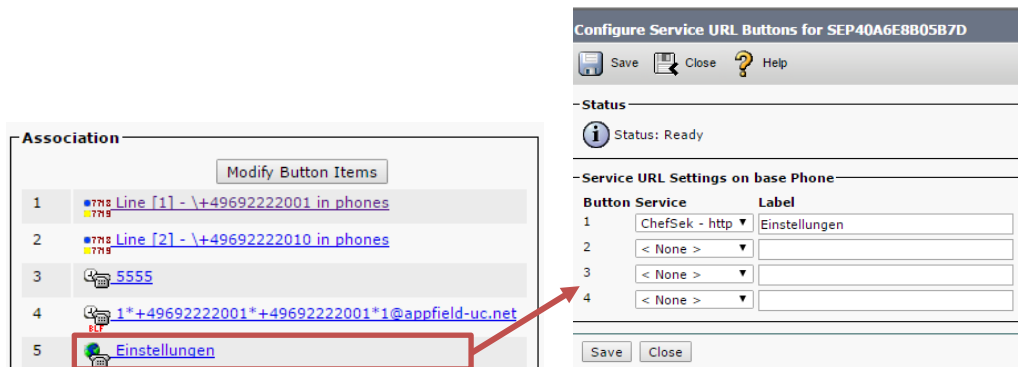


Figure 42: NFChefSek – XML Service Subscription

2.1.5.2 ASSIGN EXTERNAL CALL CONTROL PROFILE

In CUCM navigate to Device / Phone. Now search for the Manager Phone. Select the Directory Number of the Manager and set the configured ECCP to the DN:

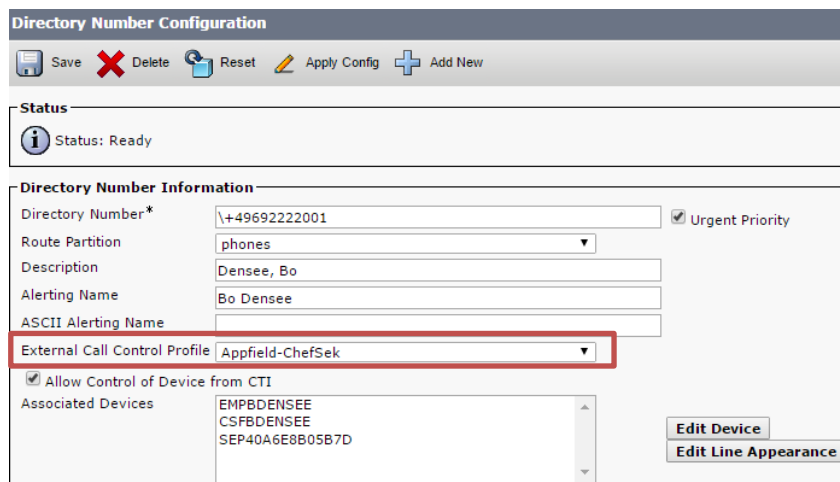


Figure 43: NFChefSek – External Call Control Profile on DN

Make sure to assign the ECCP Profile **only to the Managers**, as Assistants must not have this profile set.

2.1.5.3 APPFIELD UC – SUBSCRIBE CSS

A prerequisite when using Busy Lamp Features is to assign a Subscribe CSS that is able to access the SIP Route Pattern using a CSS/Partition.

Please make sure to assign a valid Subscribe CSS on the IP Phone (Device / Phone) and when using Extension Mobility on User / Enduser to allow BLF subscriptions.

2.1.5.4 APPFIELD UC - BLFS

Before configuring BLFs for NFChefSek you should be aware of some considerations:

- Make sure the device protocol is SIP.
- Configuring BLFs is not optional, but highly recommended due to ease of use for Managers and Assistants.
- You can decide depending on your requirements which function should be set on a dedicated BLF or not. As always there's a tradeoff between available buttons on the device and needed functions with direct access. A manager may rarely be interested in having more advanced functions in direct access, so it should be sufficient to have so having a "Diversion to Secretary" button only. While an Assistant would also like to have a BLF for "Diversion to Proxy" function.

The following functions may be controlled by a dedicated BLF:

- Diversion to Secretary (Umleitung Sekretariat), which means that all calls will be routed to configured secretaries.
- Diversion to Proxy (Vertretung) provides the ability to route calls to another colleague which is then allowed to transfer calls back to the manager.
- Pause (or Logout) is useful in environments with multiple secretaries.
- Manager-Forwarding, provides a forwarding to the configured destination instead of directly to the Manager's IP Phone. This forwarding is set in Appfield UC application logic and not a CUCM call forwarding, so it will not appear on the Managers phone display.

To use the functions specified above you have to navigate in CUCM to Device / Phone. Now search for the Manager or Assistants Phone.

- Make sure to select a Phone Button Template with sufficient BLFs configured.
- Assign the BLFs for Manager's or Assistants phone according to the logic below:

Function	BLF Destination
Diversion to Secretary (Umleitung Sekretariat)	1*(ManagerDN)*(localDeviceDN)*(Device-#)@appfield-uc.net
Diversion to Proxy (Vertretung)	2*(ManagerDN)*(localDeviceDN)*(Device-#)appfield-uc.net
Pause (Logout)	3*(ManagerDN)*(localDeviceDN)*(Device-#)@appfield-uc.net
Manager Forwarding (Chef Umleitung)	4*(ManagerDN)*(localDeviceDN)*(Device-#)@appfield-uc.net

Parameters of BLF Destination:

ManagerDN	Is the (primary) DirectoryNumber configured in Appfield UC. Which must be equal to the DN configured on the IP Phone.
localDeviceDN	Is the (primary) DirectoryNumber configured on the IP Phone where you actually configure the BLF.
Device-#	If a Manager or Assistant has multiple IP Phones with BLFs , this parameter is used to identify the device. By default this parameter is 1 (for the first IP Phone), just increment if multiple phones with identical DN belong to the same Manager.

Below you'll find a sample BLF configuration for a Manager. The manager has a single "Appfield BLF", which is used to Enable or Disable Diversion to Secretary.

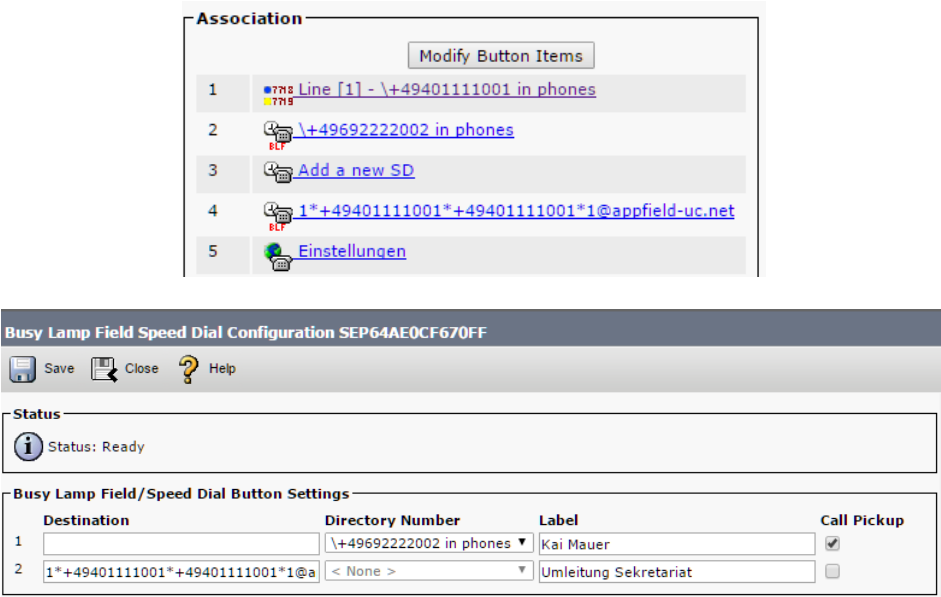
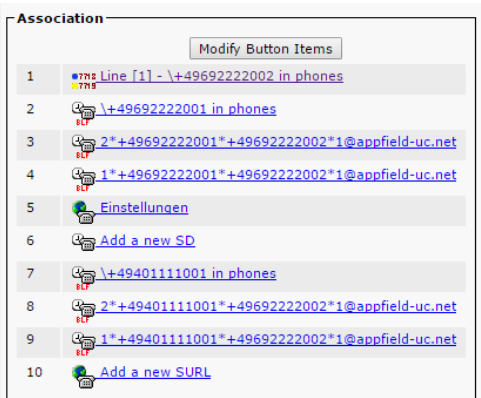


Figure 44: NFChefSek – Sample BLF Configuration - Manager

Below you'll find a sample BLF configuration for an Assistant. The assistant has four "Appfield BLF" and is able to serve 2 managers. For each manager a "Diversion to Secretary" and "Diversion to Proxy" feature has been implemented.



Status

Status: Ready

Busy Lamp Field/Speed Dial Button Settings

	Destination	Directory Number	Label	Call Pickup
1		\+49692222001 in phones ▼	Bo Densee (Chef1)	<input checked="" type="checkbox"/>
2	2*+49692222001*+49692222002*1@a	< None > ▼	Vertretung (Sek1)	<input type="checkbox"/>
3	1*+49692222001*+49692222002*1@a	< None > ▼	Umleitung Sekretariat (Sek1)	<input type="checkbox"/>
4		\+49401111001 in phones ▼	Andi Theke (Chef2)	<input checked="" type="checkbox"/>
5	2*+49401111001*+49692222002*1@a	< None > ▼	Vertretung (Sek2)	<input type="checkbox"/>
6	1*+49401111001*+49692222002*1@a	< None > ▼	Umleitung Sekretariat (Sek2)	<input type="checkbox"/>

Figure 45: NFChefSek – Sample BLF Configuration - Assistant


2.2 NFCHEFSEK CONFIGURATION


To configure NFChefSek App, please follow the instructions below. **Before proceeding make sure that you have completed configurations in chapter 2.1.**


2.2.1 BASE CONFIGURATION

In this chapter we are able to set general configuration settings.


Settings


NFOffice Integration:  ☒


Enable SIP BLF Feature:  ☒

SIP Port: 

SIP Trunk Name: 

Hide Hlog Button:  ☒

Disable Sip Cancel Status Code:  ☐

Phone Service Refresh Timer: 

Save Settings

Service » NFChefSek

Configuration Secretaries Log

App Settings

Enable SIP BLF Feature: ⓘ ☒

SIP Port: ⓘ 5060

Phone Service Refresh Timer: ⓘ 30

Disable http Access: ⓘ ☐

Save Settings

CUCM IP Phone Services Configuration

Service URL http://172.16.10.104/NFChefSek/App?DeviceName=#DEVICENAME#

Service Category XML-Dienst

Service Type Standard-IP-Telefondienst

Busy Lamp Fields

- 1*(Chef DN)*(Sek DN)*(Geräteanzahl)@appfield-uc.net (ChefSek AN/AUS)
- 2*(Chef DN)*(Sek DN)*(Geräteanzahl)@appfield-uc.net (Sekretariat Weiterleitung AN/AUS)
- 3*(Chef DN)*(Sek DN)*(Geräteanzahl)@appfield-uc.net (Pause AN/AUS)
- 4*(Chef DN)*(Sek DN)*(Geräteanzahl)@appfield-uc.net (Chef Weiterleitung AN/AUS)

Die Geräteanzahl startet bei 1 und erhöht sich bei einer weiteren Konfiguration eines Gerätes der Sekretärin um eins!

CURRI Service URL http://172.16.10.104:80/NFChefSek/CallRouting

Figure 46: NFChefSek – Base Configuration

The parameters are explained below:

Parameter	Description
Enable SIP BLF Feature	Enable the SIP feature for ChefSek to set status informations using BLFs.
SIP Port	Enter the port (TCP) used on CUCM to listen and send SIP messages on the configured SIP trunk.
Phone Service Refresh Timer	Set the refresh timer for updating the XML service page automatically.
Disable http Access	This option, when set to true, disables http (port 80) access to Appfield UC for the specified App. When set to true only https (port 443) is available. Make sure to trust the certificate in CUCMs OS configuration (tomcat-trust truststore) for IP-Phones. For Jabber clients verify that Appfield Manager certificate is trusted by client's OS truststore. When using LSCs make sure to import CAPF certificate chain into Appfield Mangers truststore.

For more information's on security Configurations please refer to chapter 1.3.4.

Service » NFChefSek

Configuration
Help
Application
Log

CUCM Configuration

Service URL	https://172.16.10.106/NFChefSek/App?DeviceName=#DEVICENAME#
Service Category	XML-Service
Service Type	Standard-IP-Telefondienst
Busy Lamp Fields	<ul style="list-style-type: none"> 1*(Chef DN)*(Device DN)*(Device count)@appfield-uc.net (Chef/Sec ON/OFF) 2*(Chef DN)*(Device DN)*(Device count)@appfield-uc.net (Secretary forward ON/OFF) 3*(Chef DN)*(Device DN)*(Device count)@appfield-uc.net (Pause ON/OFF) 4*(Chef DN)*(Device DN)*(Device count)@appfield-uc.net (Chef forward ON/OFF) <p>You have to increment the device count, by adding a device for existing secretary. Only necessary if a user has multiple devices to unique identify the device.</p>
CURRI Service URL	https://172.16.10.106:443/NFChefSek/CallRouting

Figure 47: NFChefSek – URL Configuration (Helppage)

2.2.2 SECRETARY CONFIGURATION

In this chapter we are able to set general configuration settings.

Secretary Entry

Manager Display Name: Bo Densee

Enable Diversion to Secretary:

Manager DN (Directory Number): +49692222001

Diversion Number to Secretary: +49692222002

Enable Manager Forwarding:

Number for Manager Forwarding: +4915161331077

Enable Diversion to Proxy:

Proxy DN (Directory Number): +49401111001

Members:

1
✖
Directory Number: +49692222002
Assistant Display Name: Kai Mauier
Active:

2
✖
Directory Number: +49401111001
Assistant Display Name: Andi Theke
Active:

Add item

Whitelist:
Add item

Blacklist:
Add item

Save Secretary
Delete Secretary

Figure 48: NFChefSek – Base Configuration

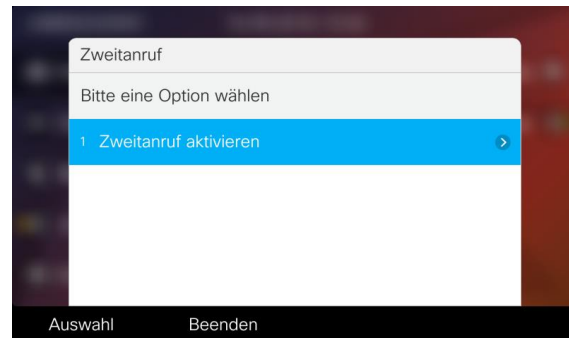
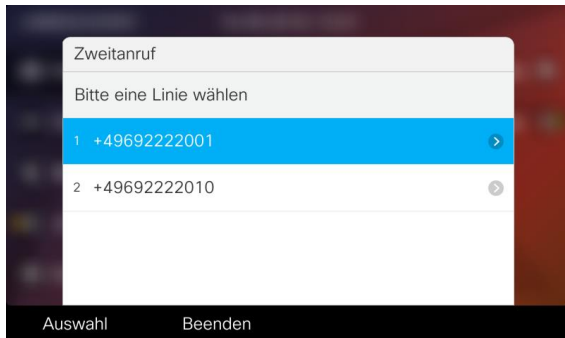
Parameter	Description
Manager Display Name	Enter the Managers Name that will show up in XML Service and NFOffice UC webtab.
Enable Diversion to Secretary	This parameter enables diversion to the secretary, as specified in "Diversion Number to Secretary" field.
Manager DN (Directory Number)	Specify the primary DN of the manager as configured in CUCM (do not use "\" when using E164 DNs)
Diversion Number to Secretary	When "Enable Diversion to Secretary" is set to true, a call to the Manager DN is diverted to the phone number specified in this field. You can either select a secretary phone directly or specify a hunt pilot that provided advanced call distributions to multiple secretaries.
Enable Manager Forwarding	This parameter sets the call forward to the "Number for Manager Forwarding". The target may be any number, like a Managers mobile phone, in a dialable format.
Number for Manager Forwarding	When "Enable Manager Forwarding" is set to true, is a call that is placed to the manager DN is diverted to the phone number specified in this field. When "Enable Diversion to Secretary" is true, only secretary calls will reach the specified number.
Enable Diversion to Proxy	This parameter enables that calls to the Manager DN are diverted to the proxy, instead of the secretaries.
Proxy DN (Directory Number)	When "Enable Diversion to Proxy" is set to true, a call to the specified manager is diverted to the phone number specified in this field. The DN specified will be allowed to transfer calls back to the manager when "Enable Diversion to Proxy" parameter is set to true.
Members	Configure at least one Assistant in the members section. Having multiple members is only required for parallel (or priority) ringing of secretaries using a hunt pilot configuration in CUCM.
Whitelist	Members in this list will be able to reach the manager, regardless if diverted to a defined secretary.
Blacklist	Members in this list will never be able to reach the manager directly, regardless if diversion to secretary is active or not.

Table 5: Secretary configuration

3 NFBUSYTRIGGER

Our NFBusyTrigger App is a simple and intuitive solution to set Call Waiting (Zweitanruf) on the Cisco IP Phone, that provide the following features

- Set Call Waiting on IP Phone
- Multiple Lines per Device Supported.
- Integration with Cisco Jabber using NFOffice-UC



3.1 CUCM CONFIGURATION

This chapter provides the configuration steps needed to implement NFBusyTrigger on the CUCM.

The following list shows the required (and optional) configurations steps:

- XML Service

3.1.1 XML SERVICE

In CUCM navigate to Device / Device Settings / Phone Services and create a new phone service with the settings shown below:

- Make sure to set the HTTP(s) URL to your Appfield UC Appliance IP:

Unsecure: `http://<IP-of-AppfieldUC>/NFBusyTrigger/App?DeviceName=#DEVICENAME#`

Secure: `https://<IP-of-AppfieldUC>/NFBusyTrigger/App?DeviceName=#DEVICENAME#`

Service Information

Service Name*
Service Description
Service URL*
Secure-Service URL
Service Category*
Service Type*
Service Vendor
Service Version
☒ Enable

Service Parameter Information

Parameters

New Parameter
Edit Parameter
Delete Parameter

Figure 49: NFChefSek – XML Service

3.2 NFBUSYTRIGGER CONFIGURATION

To configure NFBusyTrigger App, please follow the instructions below.

Service » NFBusyTrigger

Configuration Log

App Settings

Disable http Access: ☐

Save Settings

CUCM IP Phone Services Configuration

Service URL	http://172.16.10.104/NFBusyTrigger/App?DeviceName=#DEVICENAME#
Service Category	XML-Dienst
Service Type	Standard-IP-Telefondienst

Figure 50: NFBusyTrigger –Configuration

The parameters are explained below:

Parameter	Description
Disable http Access	This option, when set to true, disables http (port 80) access to Appfield UC for the specified App. When set to true only https (port 443) is available. Make sure to trust the certificate in CUCMs OS configuration (tomcat-trust truststore) for IP-Phones. For Jabber clients verify that Appfield Manager

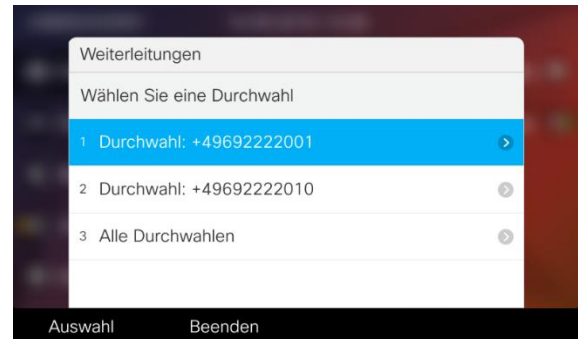
certificate is trusted by client's OS truststore. When using LSCs make sure to import CAPF certificate chain into Appfield Mangers truststore.

For more information's on security Configurations please refer to chapter 1.3.4.

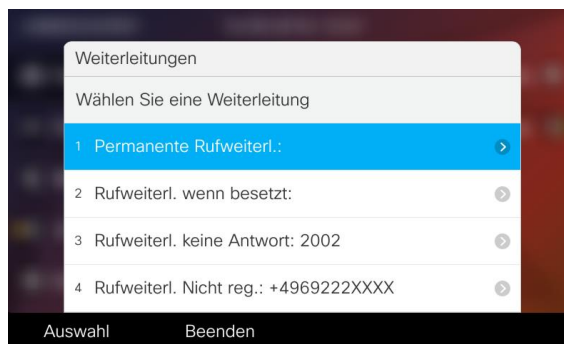
4 NFCALLFORWARDER

Our NFCallForwarder provides Call Forwarding options that are unavailable directly on IP Phones. The solution is able to set the following call forwardings:

- Call Forward - All
- CFW on Busy
- CFW on no Answer
- Set CFW no Answer Timer
- CFW on Unregistered
- CFW No Coverage
- CFW on CTI Failure



All call forward settings can be configured on a per line level or apply the configuration settings to all lines at once.



Administrator is able to select which forwardings should be offered in the XML service.

4.1 CUCM CONFIGURATION

This chapter provides the configuration steps needed to implement NFCallForwarder on the CUCM.

The following list shows the required (and optional) configurations steps:

- XML Service

4.1.1 XML SERVICE

In CUCM navigate to Device / Device Settings / Phone Services and create a new phone service with the settings shown below:

- Make sure to set the HTTP(s) URL to your Appfield UC Appliance IP:

Unsecure: `http://<IP-of-AppfieldUC>/NFCallforwarder/App?DeviceName=#DEVICENAME#`

Secure: https:// <IP-of-AppfieldUC>/ NfCallforwarder/App?DeviceName=#DEVICENAME#

The screenshot shows a configuration form for an XML service. It is divided into two main sections: 'Service Information' and 'Service Parameter Information'.

Service Information

- Service Name*: AppField NfCallforwarder
- Service Description: (empty)
- Service URL*: http://10.1.1.24/NfCallforwarder/App?DeviceName=#DEVICENAME#
- Secure-Service URL: (empty)
- Service Category*: XML-Dienst
- Service Type*: Standard-IP-Telefondienst
- Service Vendor: (empty)
- Service Version: (empty)
- ☒ Enable

Service Parameter Information

Parameters: (empty list box)

Buttons: New Parameter, Edit Parameter, Delete Parameter

Figure 51: NfCallForwarder – XML Service

4.2 NFCALLFORWARDER CONFIGURATION

To configure NfCallForwarder App, please follow the instructions below.

The screenshot shows the configuration page for the NfCallForwarder service. It includes a breadcrumb trail 'Service » NfCallforwarder' and two tabs: 'Configuration' (active) and 'Log'.

App Settings

- Show Forwarding All: ☒
- Show Forwarding Busy: ☒
- Show Forward No Answer: ☒
- Show Forward No Answer Ring Duration: ☒
- Show Forward Unregistered: ☒
- Show Forward No Coverage: ☐
- Show Forward CTI Failure: ☐
- Disable http Access: ☐

Save Settings

CUCM IP Phone Services Configuration

Service URL	http://172.16.10.104/NfCallforwarder/App?DeviceName=#DEVICENAME#
Service Category	XML-Dienst
Service Type	Standard-IP-Telefondienst

Figure 52: NfCallForwarder –Configuration

The parameters are explained below:

Parameter	Description
Show Forwarding All	Show the Call Forwarding All setting in XML service and NFOffice UC webtab.
Show Forwarding Busy	Show the Call Forwarding Busy setting in XML service and NFOffice UC webtab. This parameter applied to Busy internal and external.
Show Forward No Answer	Show the Call Forwarding No Answer setting in XML service and NFOffice UC webtab. This parameter applied to No Answer internal and external.
Show Forward No Answer Ring Duration	Show the No Answer Ring Duration parameter in XML service and NFOffice UC webtab.
Show Forward Unregistered	Show the Call Forwarding Unregistered setting in XML service and NFOffice UC webtab. This parameter applied to Unregistered internal and external.
Show Forward No Coverage	Show the Call Forwarding No Coverage setting in XML service and NFOffice UC webtab. This parameter applied to No Coverage internal and external.
Show Forward CTI Failure	Show the Call Forwarding on CTI Failure setting in XML service and NFOffice UC webtab.
Disable http Access	This option, when set to true, disables http (port 80) access to Appfield UC for the specified App. When set to true only https (port 443) is available. Make sure to trust the certificate in CUCMs OS configuration (tomcat-trust truststore) for IP-Phones. For Jabber clients verify that Appfield Manager certificate is trusted by client's OS truststore. When using LSCs make sure to import CAPF certificate chain into Appfield Mangers truststore.

For more information's on security Configurations please refer to chapter 1.3.4.

5 NFCompanyDirectory

Our NFCompanyDirectory provides a very customizable Phonebook that fits your customer needs. NFCompanyDirectory provides the following features:

- Create a Phonebook based on LDAP using:
 - MS Active Directory
 - OpenLDAP
- Define search parameters in accordance with customer requirements.
- Set search results and their layout presented on Cisco IP Phone.
- Show any LDAP parameters like Mobile, eMail, Departments, etc.
- Make a parameter dialable, whatever LDAP field it is.
- Set filter criteria on LDAP to ensure no System Users are presented in the phone book.

You may have the requirement to create multiple Directories, no problem just upload another LDAP Directory WAR File to Appfield UC and configure it.

5.1 CUCM CONFIGURATION

This chapter provides the configuration steps needed to implement NFCallForwarder on the CUCM.

The following list shows the required (and optional) configurations steps:

- XML Service

5.1.1 XML SERVICE

In CUCM navigate to Device / Device Settings / Phone Services and create a new phone service with the settings shown below:

- Make sure to set the HTTP(s) URL to your Appfield UC Appliance IP:

Unsecure: `http://<IP-of-AppfieldUC>/NFCompanyDirectory/App?DeviceName=#DEVICENAME#`

Secure: `https:// <IP-of-AppfieldUC>/ NFCompanyDirectory /App?DeviceName=#DEVICENAME#`

Service Information	
Service Name*	Appfield NFCompanyDirectory
Service Description	
Service URL*	http://10.1.1.24/NFCompanyDirectory/App?DeviceName=#DEV;
Secure-Service URL	
Service Category*	XML-Dienst
Service Type*	Verzeichnisse
Service Vendor	
Service Version	
<input checked="" type="checkbox"/> Enable	

Service Parameter Information	
Parameters	<div><div></div><div>New Parameter Edit Parameter Delete Parameter</div></div>

Figure 53: NFCompanyDirectory – XML Service

5.2 NFCOMPANYDIRECTORY CONFIGURATION

To configure NfCompanyDirectory App, please follow the instructions below.

Service » NfCompanyDirectory

ConfigurationLog

App Settings

LDAP Server IP: 10.1.1.40

LDAP Port: 389

LDAP Search Base: OU=Mitarbeiter,DC=netfarmers,DC=net

LDAP Manager DN: CN=Appfield LDAP,CN=Users,DC=netfarmers,DC=net

LDAP Password: cisco123!

LDAP Custom Filter: objectclass=*

LDAP Fields in Search page:

1

LDAP Attribute: sn

Attribute Display Name: Nachname

2

LDAP Attribute: givenName

Attribute Display Name: Vorname

Add item

LDAP Fields in Contact Details:

1

LDAP Attribute: sn

Attribute Display Name: Nachname

LDAP Field is a dialable number: ☐

2

LDAP Attribute: givenName

Attribute Display Name: Vorname

LDAP Field is a dialable number: ☐

3

LDAP Attribute: Phone

Attribute Display Name: Telefon

LDAP Field is a dialable number: ☒

4

LDAP Attribute: Mobile

Attribute Display Name: Handy

LDAP Field is a dialable number: ☒

5

LDAP Attribute: userPrincipalName

Attribute Display Name: E-Mail

LDAP Field is a dialable number: ☐

Add item

LDAP Fields in Results page: {sn}<,>{givenName}<
 <{userPrincipalName}

detailPromtFormat: {userPrincipalName}

detailTitleFormat: {sn}<,>{givenName}

Disable http Access: ☐

Save Settings

Figure 54: NfCompanyDirectory –Configuration

The parameters are explained below:

Parameter	Description
LDAP Server IP	Enter the IP of the LDAP Server.
LDAP Port	Enter the Port of the LDAP Server.
LDAP Search Base	Enter the Search Base of the LDAP Server, this is where search will start recursively. Example: CN=Users,DC=netfarmers,DC=net
LDAP Manager DN	Enter the Distinguished Name of the user, that provides access to LDAP Server. Example: CN=appfieldldapuser,CN=Users,DC=netfarmers,DC=net
LDAP Password	Enter the password of the specified user.
LDAP Custom Filter	Specify a filter for not displaying system or non visible users. Example: (&(objectclass=user)(telephonenumber=*))
LDAP Fields in Search page	In this section you can define all attributes, that may be used to search for contacts.
LDAP Attribute	Specify the name of the attribute in your LDAP directory. Example: sn, givenName, telephoneNumber
Attribute Display Name	Specify the name to display the attribute, e.g. Firstname
LDAP Fields in Results page	In this section you can define all attributes, that will be displayed in the results page. Example: {sn},,;{givenName};;{telephoneNumber};\n;{mail} Adjust the values to your requirements. Use {} to specify the ldap attribute. Use ; for separation. Use \n for carriage return.
LDAP Fields in Contact Details	In this section you can define all attributes, that will be displayed when selecting the contact from results page. Make sure that displayFields contain at least all fields in "LDAP Fields in Results page".
LDAP Field is a dialable number	Select if the specified attribute is a dialable number or not. Example: The LDAP attribute "telephoneNumber" is typically a dialable number field.
detailPromtFormat	{sn}<>, <>{givenName}<>
 <>{userPrincipalName}
detailPromtFormat	{sn}<>, <>{givenName}
Disable http Access	This option, when set to true, disables http (port 80) access to Appfield UC for the specified App. When set to true only https (port 443) is available. Make sure to trust the certificate in CUCMs OS configuration (tomcat-trust truststore) for IP-Phones. For Jabber clients verify that Appfield Manager certificate is trusted by client's OS truststore. When using LSCs make sure to import CAPF certificate chain into Appfield Managers truststore.

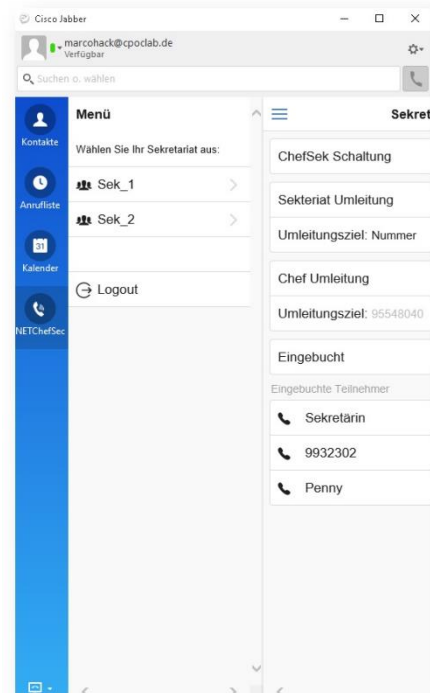
For more information's on security Configurations please refer to chapter 1.3.4.

6 NFOFFICE-UC

Our NFOffice UC is our interface to Cisco Jabber application. We use Webtabs in Cisco Jabber to provide access to our NF Apps.

The following NF Apps can be controlled by the user using NFOffice UC:

- NFChefSek
- NFBusyTrigger
- NFCallForwarder



6.1 CUCM CONFIGURATION

This chapter provides the configuration steps needed to implement NFOffice UC on the CUCM.

The following list shows the required (and optional) configurations steps:

- Custom Jabber Tab

6.1.1 CUSTOM JABBER TAB

WebTabs in Cisco Jabber are defined in the configuration file jabber-config.xml. If you would like to provide NFOffice UC to your users, you can distribute the NFOffice UC webtab to your Cisco Jabber application.

The following snippet is a configuration sample for NFOffice UC webtab, please insert the section into your jabber-config.xml:

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
  <Client>
    <jabber-plugin-config>
      <browser-plugin>
        <page refresh="false" preload="true">
```

```

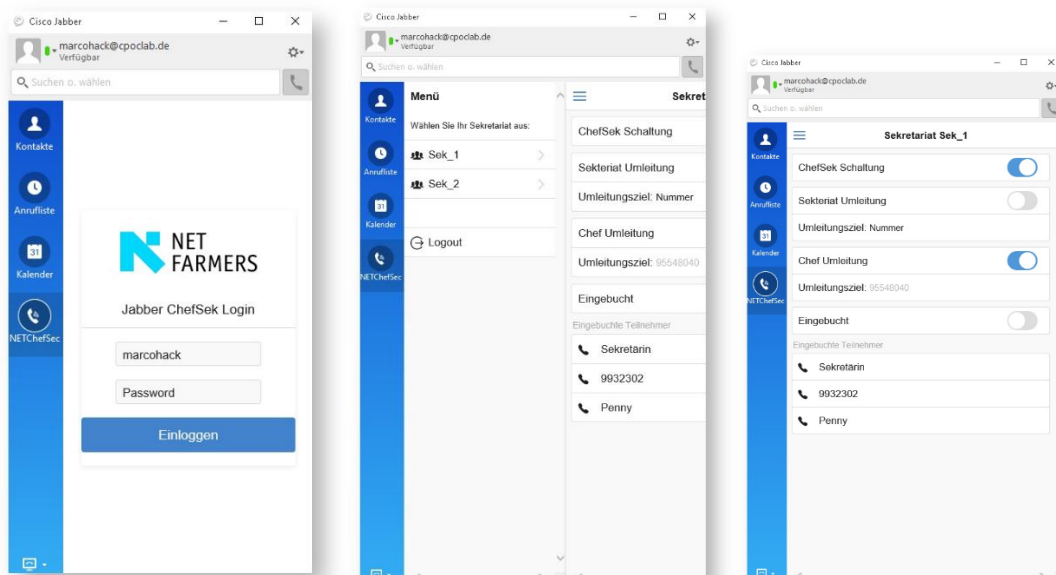
<tooltip>OfficeUC</tooltip>
<icon>http://<ApplianceIP>/NFOfficeUC/favicon-32x32.png</icon>
<url>http://<ApplianceIP>/NFOfficeUC/App?userID=${UserID}</url>
</page>
</browser-plugin>
</jabber-plugin-config>
</Client>
</config>

```

In the URL of NFOffice UC we do use a Jabber specific configuration parameter `${UserID}`, which automatically adds the UserID to into the login screen of NFOffice UC. After updating Cisco Jabber Config File please make sure to restart Cisco TFTP service in CUCM.

*For testing purposes you can alternatively copy jabber-config.xml to your local PC and replace the existing file in the path:
 C:\Users\<Benutzername>\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF\Config.*

To make the Webtab available please restart Cisco Jabber. The Webtab should now show up and you can login with your CUCM Password.



In order to use NFOffice UC App while using Mobile Remote Access you have to configure Cisco Expressway to support HTTP Webproxy forwarding to Appfield UC. On Cisco Expressway-C Node please configure the HTTP Allow List as shown in the figure:

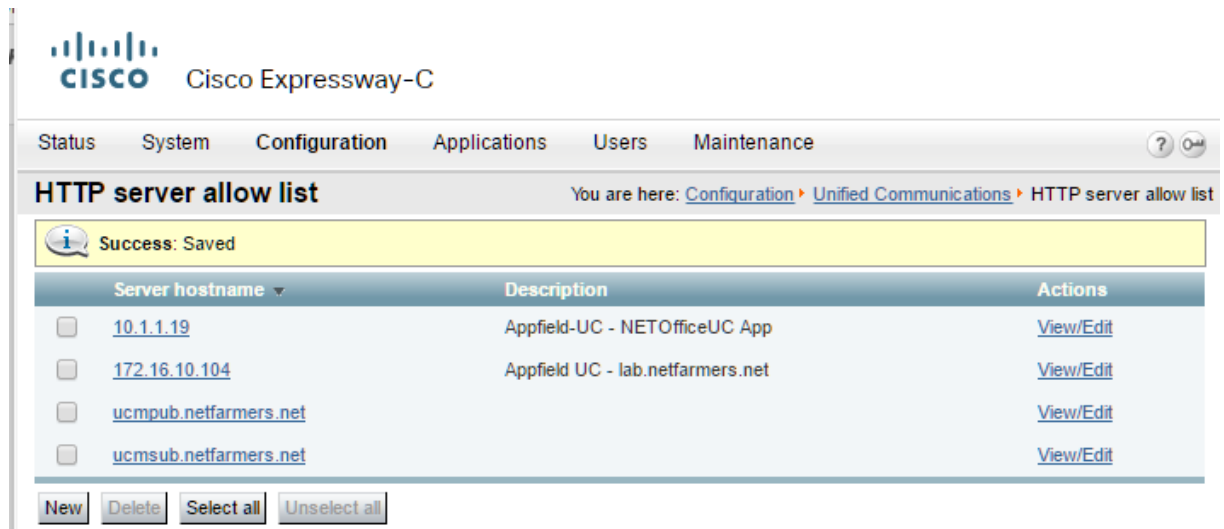


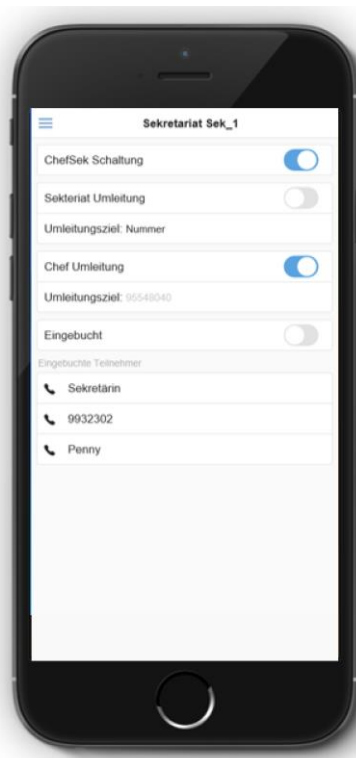
Figure 55: MRA – HTTP Allow List

As only Cisco Jabber for Desktop support embedded Webtabs, NFOffice UC with MRA is only supported on Cisco Jabber for Desktop. However you are able to use NFOffice UC on mobile devices, when you are able to reach Appfield appliance via IP (e.g. using Cisco Anyconnect VPN connection).

6.1.3 MOBILE DEVICE INTEGRATION

NFOffice UC App supports mobile device to provide Smartphones or Tablets access to NFOffice UC. You need to make sure that IP connectivity to Appfield appliance is available. On the mobile device browser open the following URL:

`https://<FQDN_of_Appfield>/NFOfficeUC/App`

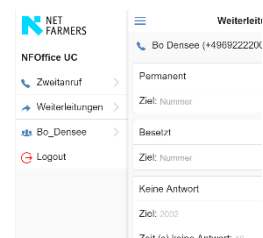


Next you'll find online configuration guidelines on how to add the NOffice UC to the Home Screen on the Smartphone or Tablet device.

- iOS: <http://www.apple.com/chde/ios/add-to-home-screen/>
- Android: <http://mobile-pixels.com/pin-webapp-website-android-homescreen/>

6.2 NFOFFICE UC CONFIGURATION

To configure NOffice UC App, please set the Service Names as configured in Appfield UC appliance. If the Service Name is leaved blank then the feature is disabled in NOffice. Otherwise the active services are shown in the navigation sidebar.



The parameters are explained below:

Parameter	Description
Service Name for ChefSek	Enter the service name for ChefSek, as shown on Services page (column Service) to enable this service in NOffice UC webtab.
Service Name for BusyTrigger	Enter the service name for BusyTrigger as shown on Services page (column Service) to enable this service in NOffice UC webtab.
Service Name for Callforwarder	Enter the service name for CallForwarder as shown on Services page (column Service) to enable this service in NOffice UC webtab.

Disable http Access

This option, when set to true, disables http (port 80) access to Appfield UC for the specified App. When set to true only https (port 443) is available. Make sure to trust the certificate in CUCMs OS configuration (tomcat-trust truststore) for IP-Phones. For Jabber clients verify that Appfield Manager certificate is trusted by client's OS truststore. When using LSCs make sure to import CAPF certificate chain into Appfield Mangers truststore.

Table 6: NFOffice configuration

For more information's on security Configurations please refer to chapter 1.3.4.

6.3 SAML SSO CONFIGURATION

NFOfficeUC can be enabled to use SAML SSO login flow, instead of Username/Passwort Authentication from CUCM.

This chapter will guide you to the process to setup SAML SSO on NFAppfield Appliance and guide you through the required configuration steps on Microsoft AD FS server.

6.3.1 MICROSOFT AD FS CONFIGURATION

This chapter will guide you through the configuration process to setup the Relying Party Trusts configuration for NFOfficeUC in Microsoft AD FS.

Please note that only non-default configuration settings are shown.

Relying Party Trust Properties:

Tab: Identifiers

Please set the identifiers. We recommend using FQDN, when having an appfield cluster, use the Cluster FQDN. Depending on your configuration, you can use default https oder :8443 port usage. Typically, you'll need only a single entry, like:

`https://appfieldha.lab.netfarmers.net:8443/NFOfficeUC/saml`

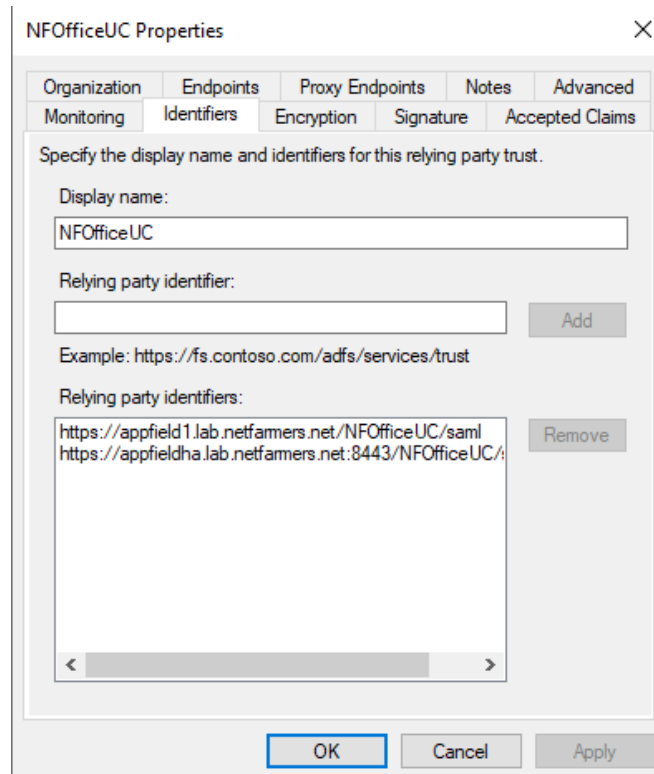


Figure 56: NFOfficeUC – Relying Party Trust - Identifiers

Tab: Encryption & Signature

Make sure to use Appfield server certificate and import the certificate into the encryption and signature sections. You can export the Appfield server certificate in Appfield in Certificates / Installed Certificates.

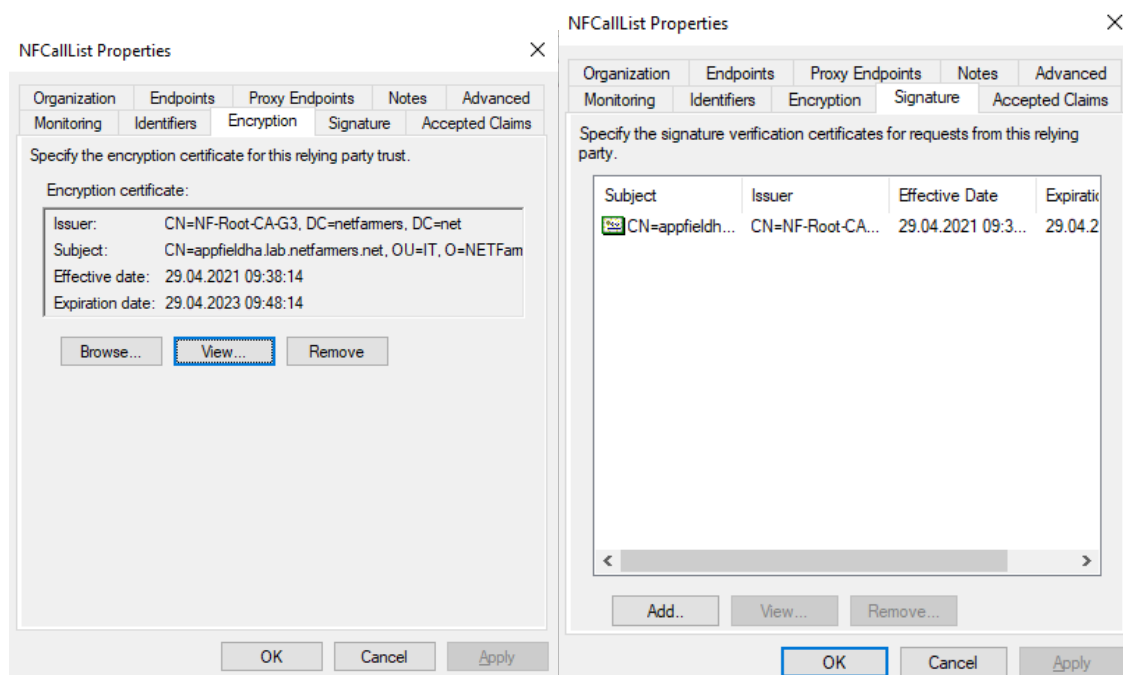


Figure 57: NFOfficeUC – Relying Party Trust – Encryption & Signature

Tab: Endpoints

On tab endpoints add the URL same URL as already used in the “Identifiers” tab, e.g.

`https://appfieldha.lab.netfarmers.net:8443/NFOfficeUC/saml`

Make sure to use the settings as shown in the right figure:

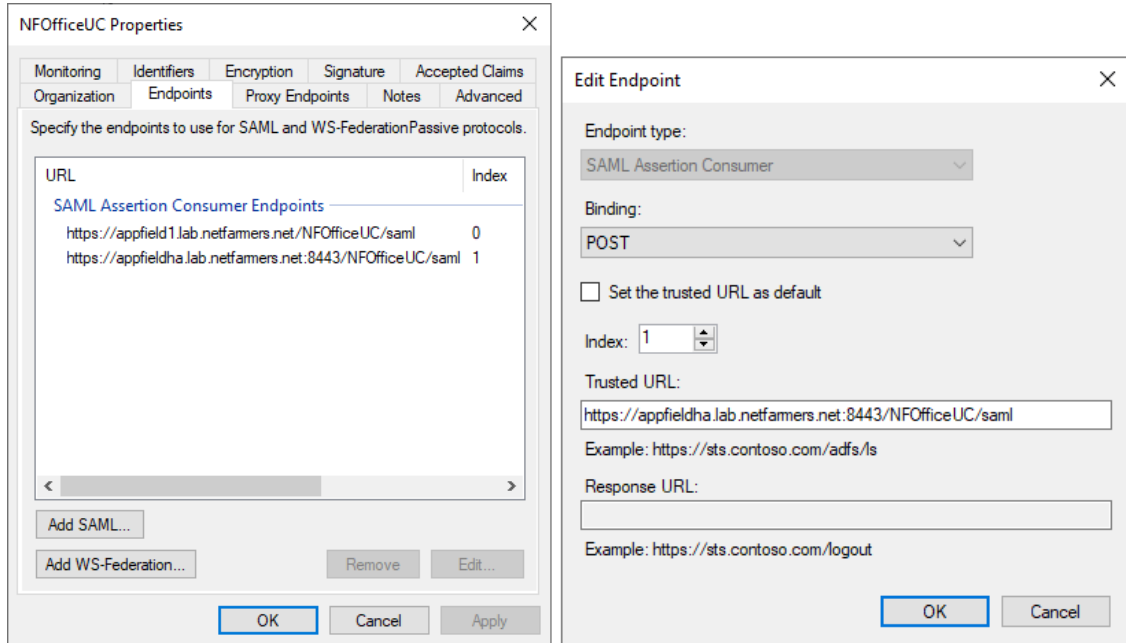


Figure 58: NFOfficeUC – Relying Party Trust – Endpoints

If you need entered multiple URLs in “Identifier” tab, you must add those here as well.

Tab: Advanced

On tab Advanced make sure to set the Secure Hash Algorithm to SHA-256.

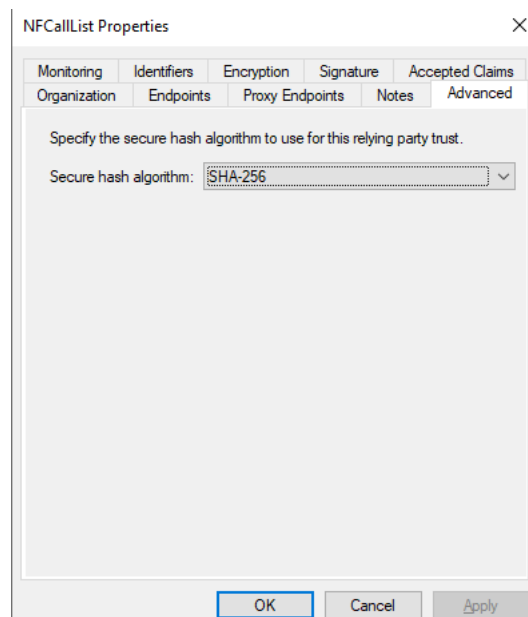


Figure 59: NOfficeUC – Relying Party Trust – Advanced

Claim Issuance Policy for Relying Party Trust:

Edit the claim issuance settings for the configured relying party trust.

Set a Claim Rule name and map the following fields accordingly:

- SAM-Account-Name -> Name ID
- Token-Groups – Unqualified Name -> Group

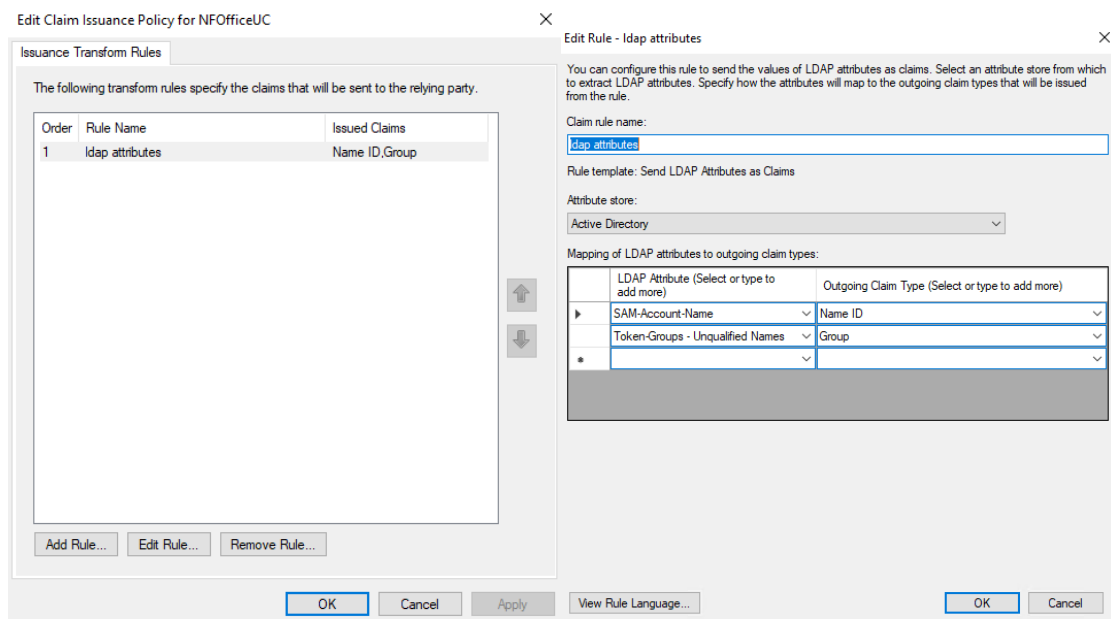


Figure 60: NOfficeUC – Claim Issuance Policy

6.3.2 APPFIELD CONFIGURATION

In Appfield the SAML SSO configuration is split into two segments.

- 1) Trust Identity Provider certificate
- 2) Global SAML SSO Configuration in NFAppfieldManager
- 3) Enable / Disable SAML SSO Login Flow in NOffice

The configuration steps 1 & 2 are identical for NOfficeUC and NCallList, so you only need to do them once.

1. Trust Identity Provider certificate:

Make sure to import the certificate of your Identity Provider (namely Microsoft AD FS) into the Appfield's trust store, as Appfield needs to trust the configured metadata URL.

2. Global SAML SSO Configuration:

The parameters are explained below.

Parameter	Description
Metadata.xml URL	<p>This is the URL to the Federation MetaData.xml File from the Identity Provider (Microsoft AD FS). You have to set the URL to the IdP in the format as seen in the example.</p> <p>To fetch the latest file from the server, enter the URL and click on the button “Renew IDP Metadata”.</p>
Authentication Lifetime	This is the value the token is valid and reauthentication needs to occur.
Sign Metadata	Enables / disables signing of MetaData Files.
Auth Request Signed	Enables / disables signing of Authentication Requests.
Disable Signature Validation	This parameter disables Signature Validation, do not check this is parameter in production systems.

Table 7: SAML SSO global configuration

3. Enable / Disable SAML SSO Login Flow in NFOfficeUC:

With this step you'll enable the SAML SSO Login Flow, so that login requests are forwarded to the configured Identity Provider.

To enable the login flow, go to NFOfficeUC / Configuration and set the Parameter “Enable ADFS” to true.

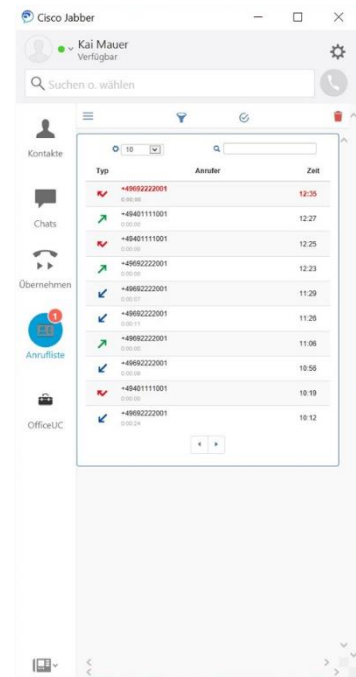
Be aware that from this point on all authentication requests are forwarded to your Identity Provider.

6.3.3 MICROSOFT AD FS TROUBLESHOOTING

Please refer to chapter 7.3.3 for further troubleshooting information's.

Our NFCallList provides a synchronized call list between Cisco Jabber and compatible Cisco IP Phones. In addition you are able to receive missed calls in status:

- While busy
- While logged out.



The figure below shows the concept of NFCallList.

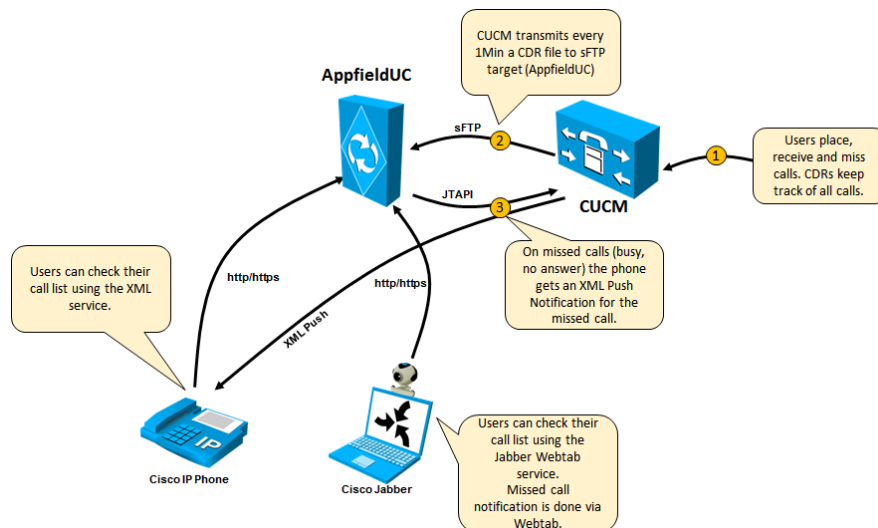


Figure 61: NFCallList – Concept

Cisco Unified Communications Manager is able to collect CDRs (1) from all calls placed, received and missed in the system. Along with multiple other information's collected in this CDR the basic data for a call log are available. All input data (2) is sent from CUCM to Appfield UC in a 1 minute interval using the CDR interface of CUCM Cluster. CDRs are sent in a csv file format and parsed into the Appfield UC database for every DN configured in CUCM, only for available DNs in CUCM are call lists created.

In case of a missed call (busy or no answer) the users of IP Phones will receive a XML Push Notification (3) on their IP Phone, which informs the user of the missed call. On Jabber the Webtab icon will show up with a red number, indicating that a missed call is available.

7.1 CUCM CONFIGURATION

This chapter provides the configuration steps needed to implement NFCallList on the CUCM.

The following list shows the required (and optional) configurations steps:

- XML Service
- Custom Jabber Tab
- CDR Management Configuration
- JTAPI User Access Rights

7.1.1 XML SERVICE

In CUCM navigate to Device / Device Settings / Phone Services and create a new phone service with the settings shown below:

- Make sure to set the HTTP(s) URL to your Appfield UC Appliance IP:

Unsecure: `http://<IP-of-AppfieldUC>/NFCallList/App?DeviceName=#DEVICENAME#`

Secure: `https:// <IP-of-AppfieldUC>/NFCallList/App?DeviceName=#DEVICENAME#`

The screenshot displays two configuration sections for a new XML service in CUCM. The top section, titled "Service Information", contains the following fields: "Service Name*" with the value "Anrufliste", "Service Description" with "NF CallList Appfield UC", "Service URL*" with "http://172.16.10.104/NFCallList/App?DeviceName=#DEVICENAME#", "Secure-Service URL" (empty), "Service Category*" set to "XML Service", "Service Type*" set to "Directories", "Service Vendor" (empty), and "Service Version" (empty). An "Enable" checkbox is checked. The bottom section, titled "Service Parameter Information", features a "Parameters" list box (currently empty) and three buttons: "New Parameter", "Edit Parameter", and "Delete Parameter".

Figure 62: NFCallList – XML Service

7.1.2 CUSTOM JABBER TAB

WebTabs in Cisco Jabber are defined in the configuration file jabber-config.xml. If you would like to provide NFCallList to your users, you can distribute the NFCallList webtab to your Cisco Jabber application.

The following snippet is a configuration sample for NFCallList webtab, please insert the section into your jabber-config.xml:

```
<?xml version="1.0" encoding="utf-8"?>
<config version="1.0">
  <Client>
    <jabber-plugin-config>
      <browser-plugin>
        <page refresh="false" preload="true">
          <tooltip>Anrufliste</tooltip>
          <icon>http://<ApplianceIP>/NFCallList/img/icon.png</icon>
          <url>http://<ApplianceIP>/NFCallList/WebApp?userID=${UserID}</url>
        >
      </page>
    </browser-plugin>
  </jabber-plugin-config>
</Client>
</config>
```

In the URL of NFCallList we do use a Jabber specific configuration parameter \${UserID}, which automatically adds the UserID to into the login screen of NFCallList. After updating Cisco Jabber Config File please make sure to restart Cisco TFTP service in CUCM.

*For testing purposes you can alternatively copy jabber-config.xml to your local PC and replace the existing file in the path:
C:\Users\<Benutzername>\AppData\Roaming\Cisco\Unified Communications\Jabber\CSF\Config.*

To make the Webtab available please restart Cisco Jabber. The Webtab should now show up and you can login with your CUCM Password.

7.1.3 CUSTOM WEBEX TAB

Tabs in Cisco Webex App are defined in the Webex Control Hub Administration Portal, the portal they are also known as "Shortcuts". If you would like to provide NFCallList to your users, you can distribute a NFCallList shortcut to your Cisco Webex application.

Known Limitations:

Due to limitations in Webex App the following limitations apply:

- *NFCallList is unable to save cookies in Webex App, therefore users need to enter their credentials when starting Webex App. To avoid entering credentials use Microsoft AD FS (SAML SSO) Integration.*
- *Presence data in NFCallList is not available.*
- *Missed calls can't be displayed in the shortcut icon, instead users must open NFCallList to check their missed calls.*

Configuration Steps:

- To setup NFCallList for WebEx App, go to the **Webex Control Hub**.
- Switch to the Management / **Apps** section.
- Click on **"Add Shortcut"** and add the required data into the form.

Display Name: Enter a descriptive name.

URL: use the following syntax for the URL:

`https://<ApplianceFQDN>/NFCallList/WebApp`

Icon: You can select a predefined icon or download the

Appfield icon from:

`https://<ApplianceFQDN>/NFCallList/img/icon.png`

You're now ready to use your NFCallList from the Webex App.

Add shortcut

Display Name *
NFCallList

URL *
https://<Appfield-FQDN>/NFCallLi

Favicon *
Select an icon or upload an image to represent this shortcut in the Webex app.

☒ Select predefined icon

Icon
Globe icon

Color
Dark blue

☐ Upload custom image
300 x 300 px transparent PNG. Max size 1 MB. Ensure the icon is visible on a dark and light background.

Cancel Save

7.1.4 CDR ENABLEMENT

In CUCM navigate to Cisco Unified Communications Manager and go to System / Service Parameters. Now select the Publisher node and select CallManager service from the list.

Make sure to set the following CUCM Parameters accordingly:

- CDR Enabled Flag: True
- CDR Log Calls with Zero Duration Flag: True

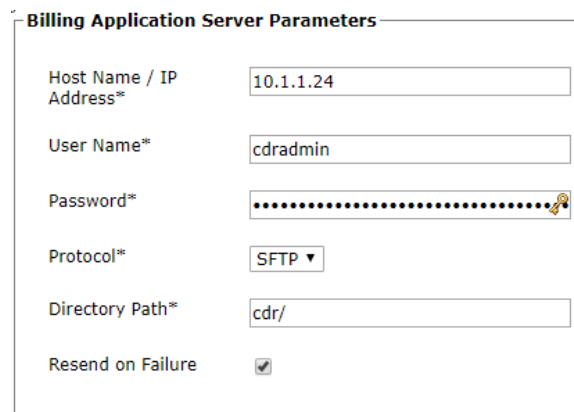
Please make sure to repeat the configuration steps above **for every CUCM node in the cluster**.

7.1.5 CDR MANAGEMENT CONFIGURATION

In CUCM navigate to Cisco Unified Serviceability and go to Tools / CDR Management. Now add a new Billing Application Server to the list, with the settings shown below:

- Hostname / IP Address: IP of Appfield UC Appliance
- User Name: cdrradmin
- Password: <as configured in CLI, default is cdrradmin>
- Protocol: SFTP
- Directory Path: cdr/
- Resend on Failure checked

Please find a sample configuration below, where the Appfield 's Appliance is 10.1.1.24:



The screenshot shows a web form titled "Billing Application Server Parameters". It contains the following fields and values:

Field	Value
Host Name / IP Address*	10.1.1.24
User Name*	cdrradmin
Password*	[Masked with dots]
Protocol*	SFTP
Directory Path*	cdr/
Resend on Failure	<input checked="" type="checkbox"/>

Figure 63: Billing Server Configuration

7.1.6 JTAPI USER ACCESS RIGHTS

For NFCallList to send Push Notifications to Cisco IP Phones the Appfield Appliance needs the following access rights on an application user. You are allowed to use the identical application user as already configured in chapter 1.3.2.1.

Make sure to go to CUCM Administration and User Management / Application User. Select an existing user or create a new user.

Assign the following Access Control Groups to this user:

- Standard CTI Allow Control of All Devices
- Standard CTI Enabled

Permissions Information

Groups

- Standard CTI Allow Control of All Devices
- Standard CTI Enabled

[View Details](#)

Roles

- Standard CTI Allow Control of All Devices
- Standard CTI Enabled

[View Details](#)

Figure 64: Access Control Group Configuration JTAPI User

Due to “Standard CTI Allow Control of All Devices” ACG you do not need to assign IP-Phones or EM Profiles to the application user. You may want to restrict Push Notifications to dedicated devices, while other devices should not get Push Notifications, in such a case you have to remove “Standard CTI Allow Control of All Devices” from the list and assign IP Phones or EM Profiles manually to the application user.

7.2 NFCALLLIST CONFIGURATION

The configuration of NFCallList is done via a few configuration items and there’s no user dedicated configuration needed.

The available configuration parameters are explained below:

Parameter	Description
Use Jabber URI from UDS Directory	If enabled the jabber userID get resolved via the CUCM UDS directory. Otherwise the jabber userID is userID@domain.
Jabber Domain	Is only necessary, if previous checkbox is unchecked. Enter the Domain that is used for Jabber, e.g. netfarmers.net
Maximum Entries per Page	Enter the maximum call entries per page.
Maximum Call Entries	Enter the maximum call entries overall per CallList.
Unknown Caller Name	For calls, where no name is displayed the text entered here is shown in the CallList.
Conference Caller Name	For ad hoc conference calls, the text entered here is shown in the CallList.
Delete CDR Files	Remove CDR files after parsing. This is the recommended configuration setting. For debugging the original CDR file can be stored on filesystem.
Ignore CDR Devices	You are able to define target devices where no call log should be created, e.g. Appfield SIP Trunk for NFChefSek or Recorder Applications where a second (transparent) call is created.

Small Resolution Phones	Phones with smaller displays that do not support images, should be entered here, e.g. CP-7841.
Clear Screen after call	After placing a call from the IP Phone CallList, the XML service will be closed automatically (checked). Otherwise the service will still be shown on screen.
JTAPI Settings:	
JTAPI Service IP	Enter the IP of the CTI Manager
JTAPI Username	Enter the Username assigned with the JTAPI Push Notification rights.
JTAPI Password	Enter the Password configured for the Username specified.
JTAPI Call Notifications	Enable or Disable Notifications for XML Push.
E-Mail Settings:	
SMTP Server	Enter the SMTP Server, that is able to receive eMails.
Username	Enter the Username / eMail of the eMail account.
Password	Enter the Password configured for the Username specified.
SSL Enabled	Use SSL for sending eMails (SMTP).
Sender E-Mail	Users receiving an eMail from Appfield UC will see this eMail address as the sender.
Send Missed Call Notification E-Mails	Enable or Disable Notifications for eMail.
Missed Call E-Mail Subject	Enter the template text that will be shown in eMail subject field.
Missed Call E-Mail Text	Enter the template text that will be shown in eMail text field.
Disable http Access	This option, when set to true, disables http (port 80) access to Appfield UC for the specified App. When set to true only https (port 443) is available. Make sure to trust the certificate in CUCMs OS configuration (tomcat-trust truststore) for IP-Phones. For Jabber clients verify that Appfield Manager certificate is trusted by client's OS truststore. When using LSCs make sure to import CAPF certificate chain into Appfield Mangers truststore.
Manual UserID	Check, if the autofill option of the userID field on login to the CallList should not be filled automatically. Otherwise the userID used for Jabber Login is used.
Show Logo in Jabber	Display the Netfarmers Company Logo on Login and Menu.

Enable Delta List	If the option is activated, only calls will be displayed on user is busy or unregistered. So the NfCallList will only extend the original one from Cisco.
Call Prefix	<p>This is the call handler URI that is executed, when making a call via NfCallList.</p> <p>Defaults to CISCOTEL for Cisco Jabber.</p> <p>For using NfCallList within Webex App use tel as the handler prefix.</p>
ADFS Settings	<p>Enabled ADFS</p> <p>Enables the SAML SSO Authentication Scheme to use Microsoft AD FS for Authentication. Please make sure that Appfield and Microsoft AD FS are configured as per document in chapter 7.3.</p>

Table 8: NfCallList configuration

For more information's on security Configurations please refer to chapter 1.3.4.

7.3 SAML SSO CONFIGURATION

NfCallList can be enabled to use SAML SSO login flow, instead of Username/Password Authentication from CUCM.

This chapter will guide you to the process to setup SAML SSO on NfAppfield Appliance and guide you through the required configuration steps on Microsoft AD FS server.

7.3.1 MICROSOFT AD FS CONFIGURATION

This chapter will guide you through the configuration process to setup the Relying Party Trusts configuration for NfCallList in Microsoft AD FS.

Please note that only non-default configuration settings are shown.

Relying Party Trust Properties:

Tab: Identifiers

Please set the identifiers. We recommend using FQDN, when having an appfield cluster, use the Cluster FQDN. Depending on your configuration, you can use default https oder :8443 port usage. Typically, you'll need only a single entry, like:

<https://appfieldha.lab.netfarmers.net:8443/NfCallList/saml>

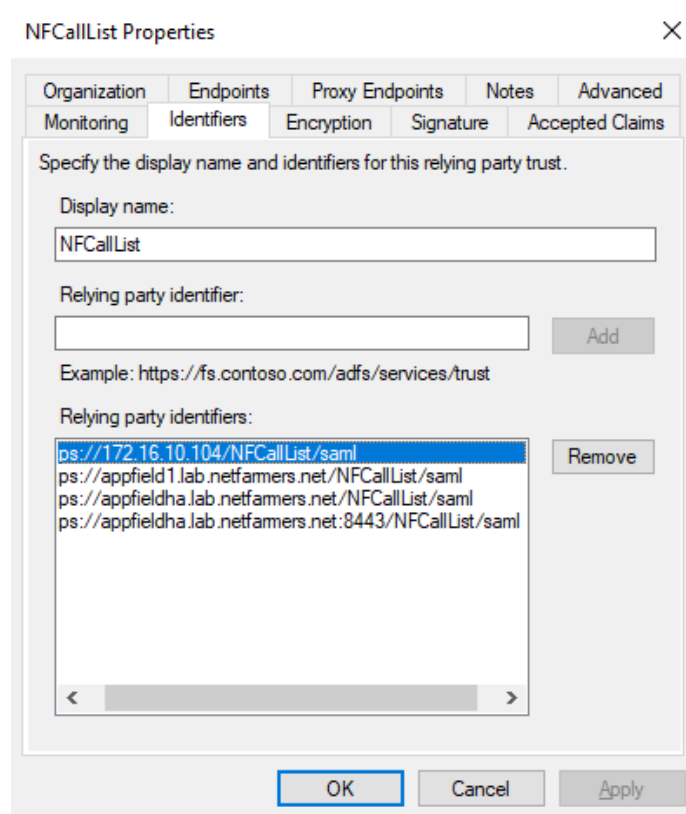


Figure 65: NFCallList – Relying Party Trust - Identifiers

Tab: Encryption & Signature

Make sure to use Appfield server certificate and import the certificate into the encryption and signature sections. You can export the Appfield server certificate in Appfield in Certificates / Installed Certificates.

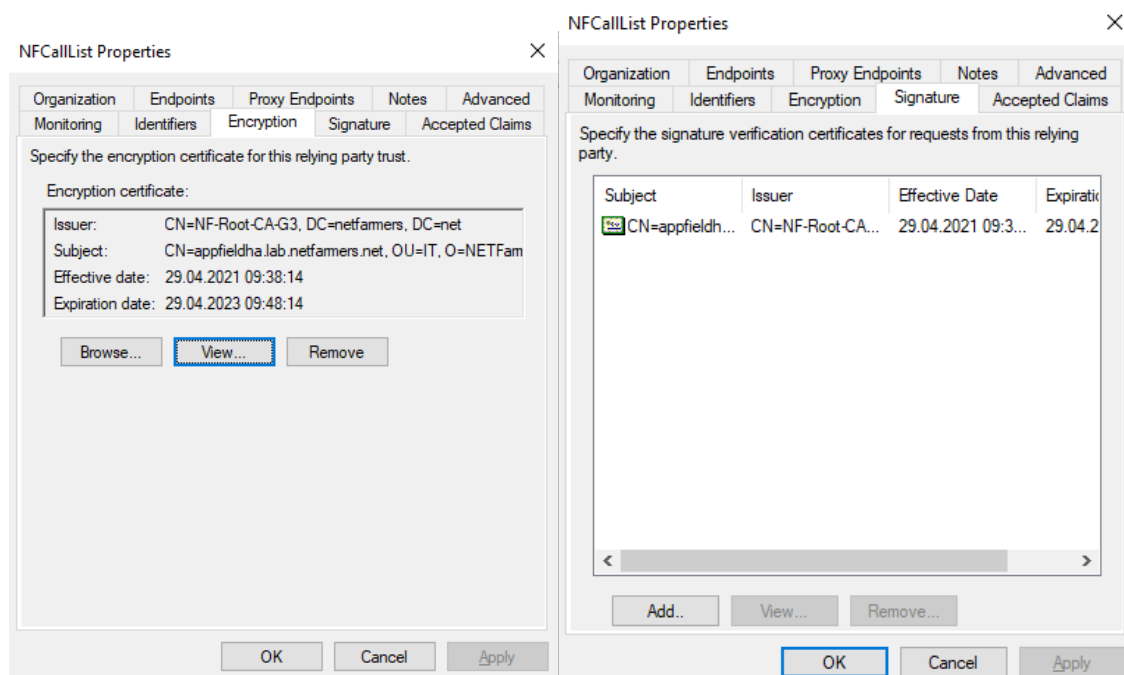


Figure 66: NFCallList – Relying Party Trust – Encryption & Signature

Tab: Endpoints

On tab endpoints add the URL same URL as already used in the “Identifiers” tab, e.g.

<https://appfieldha.lab.netfarmers.net:8443/NFCallList/saml>

Make sure to use the settings as shown in the right figure:

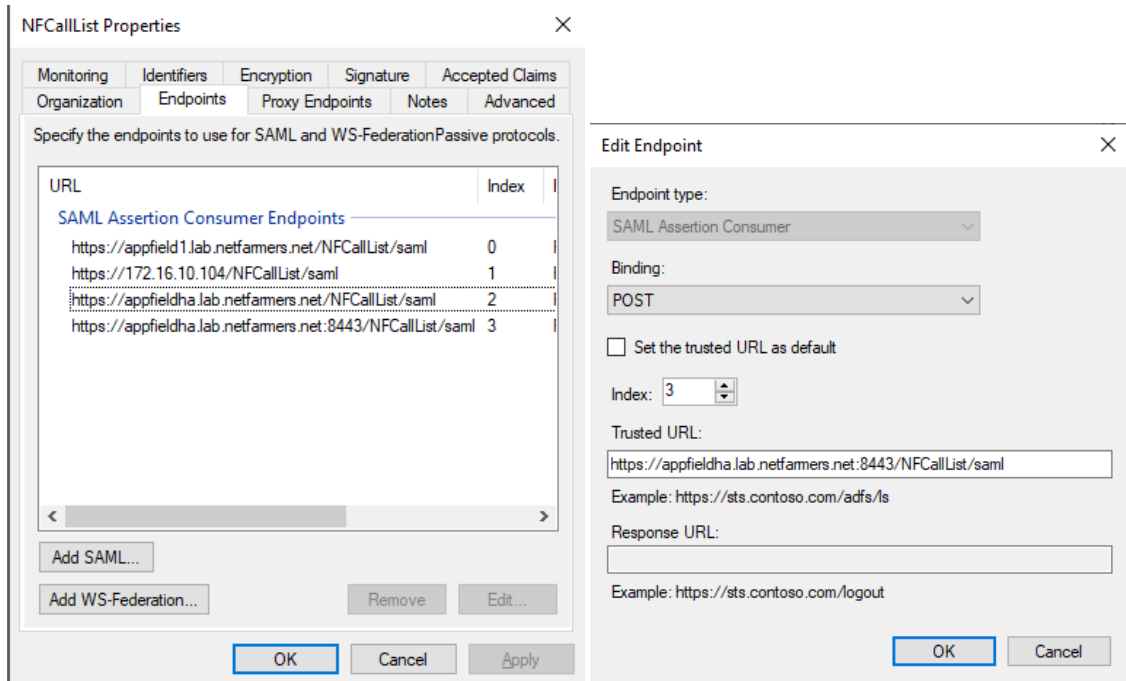


Figure 67: NFCallList – Relying Party Trust – Endpoints

If you need entered multiple URLs in “Identifier” tab, you must add those here as well.

Tab: Advanced

On tab Advanced make sure to set the Secure Hash Algorithm to SHA-245.

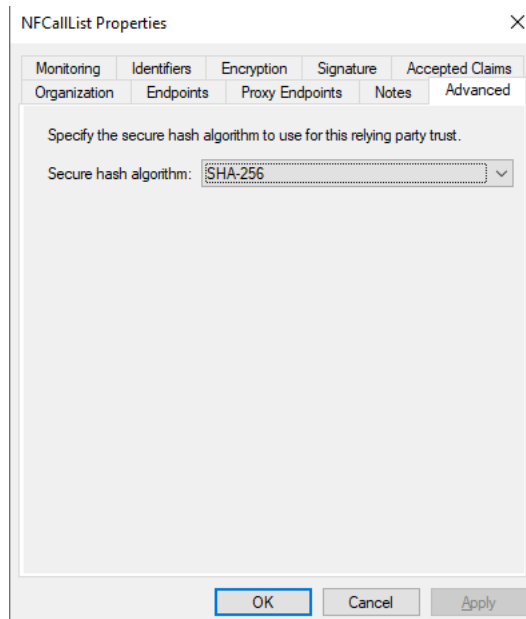


Figure 68: NfCallList – Relying Party Trust – Advanced

Claim Issuance Policy for Relying Party Trust:

Edit the claim issuance settings for the configured relying party trust.

Set a Claim Rule name and map the following fields accordingly:

- SAM-Account-Name → Name ID
- Token-Groups – Unqualified Name → Group

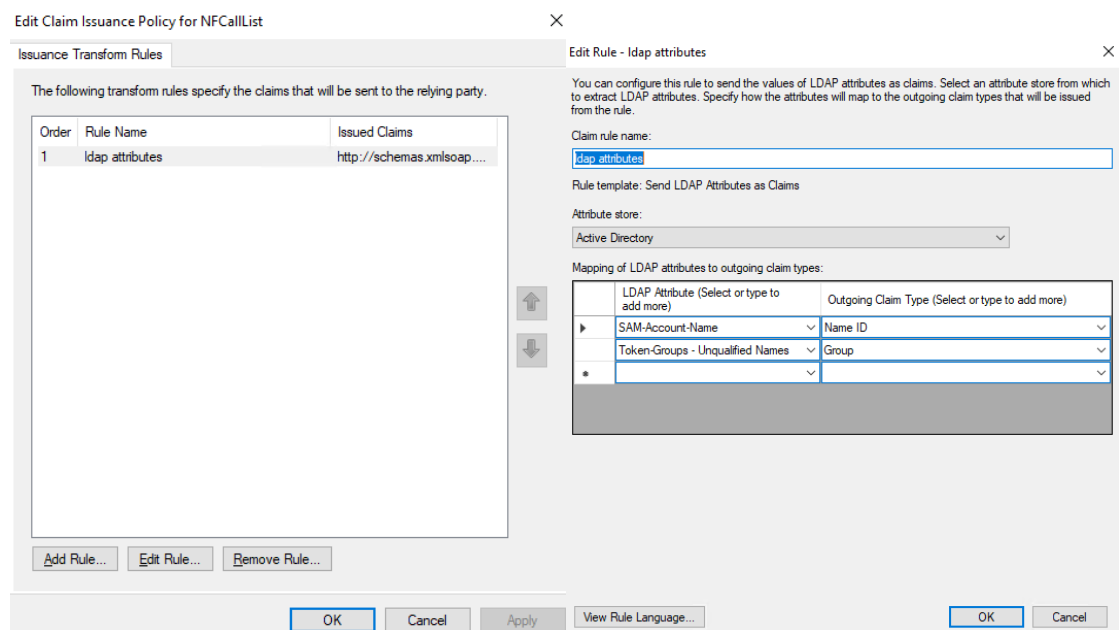


Figure 69: NfCallList – Claim Issuance Policy

7.3.2 APPFIELD CONFIGURATION

In Appfield the SAML SSO configuration is split into two segments.

- 4) Trust Identity Provider certificate
- 5) Global SAML SSO Configuration in NFAppfieldManager
- 6) Enable / Disable SAML SSO Login Flow in NFCallList

The configuration steps 1 & 2 are identical for NFOfficeUC and NFCallList, so you only need to do them once.

4. Trust Identity Provider certificate:

Make sure to import the certificate of your Identity Provider (namely Microsoft AD FS) into the Appfield's trust store, as Appfield needs to trust the configured metadata URL.

5. Global SAML SSO Configuration:

The parameters are explained below.

Parameter	Description
Metadata.xml URL	This is the URL to the Federation MetaData.xml File from the Identity Provider (Microsoft AD FS). You have to set the URL to the IdP in the format as seen in the example. To fetch the latest file from the server, enter the URL and click on the button "Renew IDP Metadata".
Authentication Lifetime	This is the value the token is valid and reauthentication needs to occur.
Sign Metadata	Enables / disables signing of MetaData Files.
Auth Request Signed	Enables / disables signing of Authentication Requests.
Disable Signature Validation	This parameter disables Signature Validation, do not check this is parameter in production systems.

Table 9: SAML SSO global configuration

6. Enable / Disable SAML SSO Login Flow in NFCallList:

With this step you'll enable the SAML SSO Login Flow, so that login requests are forwarded to the configured Identity Provider.

To enable the login flow, go to NFCallList / Configuration and set the Parameter "Enable ADFS" to true.

Be aware that from this point on all authentication requests are forwarded to your Identity Provider.

7.3.3 MICROSOFT AD FS TROUBLESHOOTING

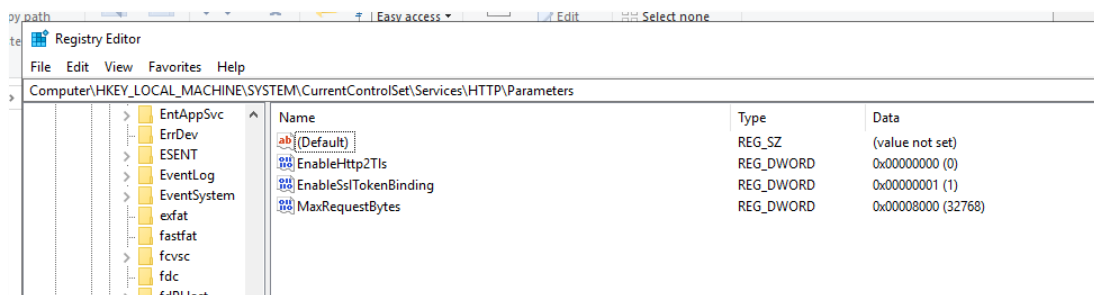
When enabling SAML SSO for Appfield we detected an issue that Microsoft AD FS is responding with a message “Bad Request – Request Too Long” (see picture below). This happens when the certificate chain of the Appfield certificate is too large for the Microsoft’s IIS servers which is used by Microsoft AD FS.

In our tests, we suspected that a certificate chain of “Root CA -> Appfield Identity Certificate” works fine , but a certificate chain of “Root CA -> SubCA1 -> SubCA2 -> SubCA3 -> Appfield Identity Certificate” will result in the error below by default:

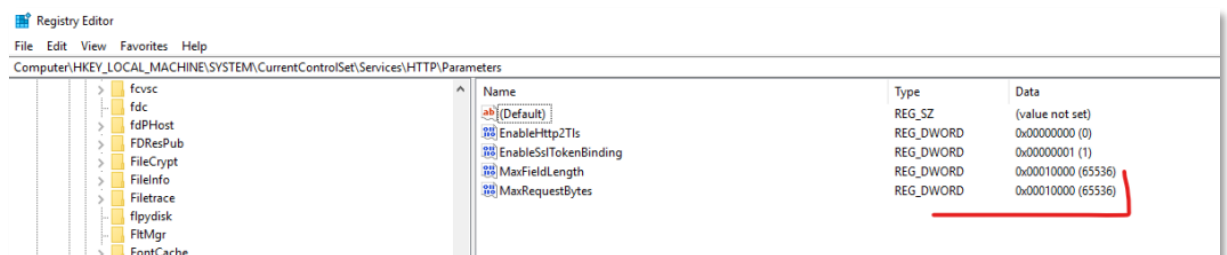


To overcome this issue Microsoft released a Troubleshooting document (<https://docs.microsoft.com/en-US/troubleshoot/developer/webapps/iis/www-administration-management/http-bad-request-response-kerberos>) the mentioned Workaround 2 is the solution for this issue here.

The default Microsoft settings on a Windows 2016 Server for MaxRequestBytes is 32768 (dec).



We increased the values to the values below and the bad request issue is solved. To apply these changes a **net stop http** and a **net start http** command is needed. Please make sure to manually start the stopped services, as Windows does not start all services, it has stopped with the **net stop http** command.



8 NCONTACTS

NContacts provides a name resolution service for Cisco IP Phones, so that external callers can be resolved with a Name (and Company Name if needed). NContacts separates between personal and global contacts.

Please note that NContacts name resolution is based on e.164 formatted numbers (e.g. +4940555222), this is the only supported numbering format.

Global contacts are resolved for all devices in a CUCM cluster, while personal contacts are only resolved for that particular user (/directory number).

Global Contact sources can be the following:

- MS Active Directory / LDAP compatible directory source
- CSV Files accessible via SMB network share.

Personal Contacts are supported using MS Exchange – Outlook Web Access (OWA) using the provided Microsoft API “EWS – Exchange Web Services”.

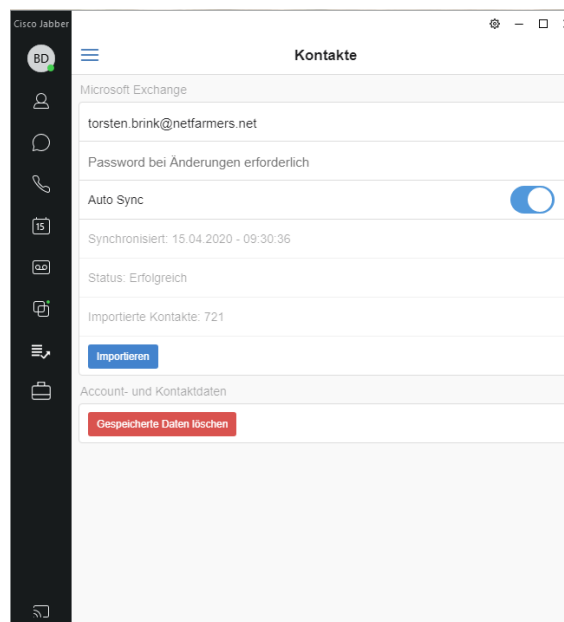


Figure 70: NOffice UC – Contacts Configuration

The user has to authenticate himself in NOfficeUC within the Contacts tab. Appfield will then contact EWS API to access the users contacts and save them in our local database. The Auto Sync Option provides a nightly sync for contacts, in case of adding/deleting contacts in MS Outlook.

- MS Exchange search results and their layout presented on Cisco IP Phone.
- Show any LDAP parameters like Mobile, eMail, Departments, etc.
- Make a parameter dialable, whatever LDAP field it is.
- Set filter criteria on LDAP to ensure no System Users are presented in the phone book.

You may have the requirement to create multiple Directories, no problem just upload another LDAP Directory WAR File to Appfield UC and configure it.

8.1 CUCM CONFIGURATION

This chapter provides the configuration steps needed to implement NFContacts on the CUCM.

The following list shows the required (and optional) configurations steps:

- External Call Control Profile
- Update/ Adjust Translation Pattern

8.1.1 EXTERNAL CALL CONTROL PROFILE

The External Call Control Profile (ECCP) is the core components to resolve names for inbound calls. The call requests are routed to Appfield, analysed and if a match has been found a name is added.

In CUCM navigate to Call Routing / External Call Control Profile and create a new External Call Control Profile with the settings as shown below.

- Make sure to set the HTTP(s) URL to your Appfield UC Appliance IP:

Mutual TLS ECCP: `https:// <IP-of-AppfieldUC>:443/NFContacts/CallRouting`

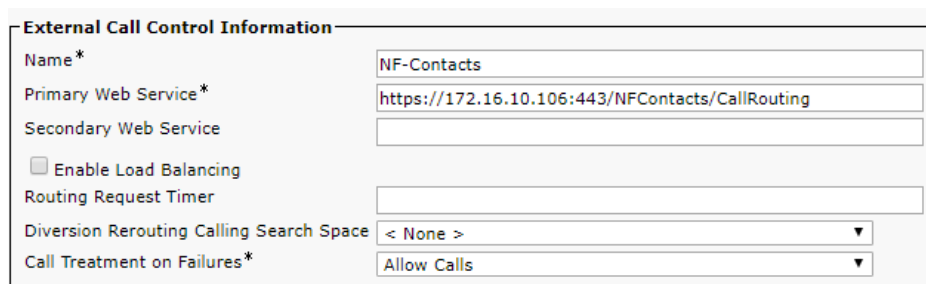
Regular TLS ECCP: `https:// <IP-of-AppfieldUC>:8443/NFContacts/CallRouting`

Note: When using 8443 make sure that Appfield Firewall settings allow port 8443, otherwise the communication will not work.

Be aware to keep the port information in the URL (e.g. :443) !!

As you can see ECCP is relying on TLS, so make sure to import each others certificates between appfield appliance and CUCM. The **callmanager-trust** truststore is used for ECCP process, so make sure to use this truststore.

- There's no need to assign a Diversion Rerouting CSS, as Appfield will never redirect calls in NFContacts.



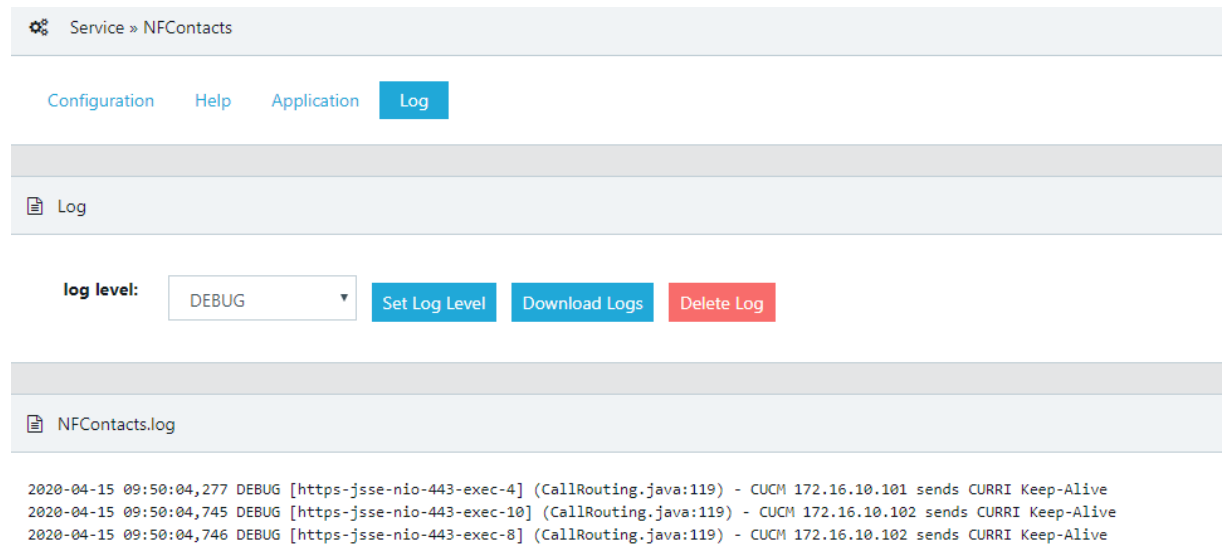
The screenshot shows the 'External Call Control Information' configuration form. The fields are as follows:

External Call Control Information	
Name*	NF-Contacts
Primary Web Service*	https://172.16.10.106:443/NFContacts/CallRouting
Secondary Web Service	
<input type="checkbox"/> Enable Load Balancing	
Routing Request Timer	
Diversion Rerouting Calling Search Space	< None >
Call Treatment on Failures*	Allow Calls

Figure 71: NFContacts – External Call Control Profile

Verification of External Call Control Profile is working

You can easily check, that NFContacts is working properly. Go to the Log section of NFContacts and set the log to Debug level. You should see CURRI Keep-Alive messages, which indicate that Appfield is receiving keepalive requests and is answering to them.



Service » NFContacts

Configuration Help Application Log

Log

log level: Set Log Level Download Logs Delete Log

NFContacts.log

```
2020-04-15 09:50:04,277 DEBUG [https-jsse-nio-443-exec-4] (CallRouting.java:119) - CUCM 172.16.10.101 sends CURRI Keep-Alive
2020-04-15 09:50:04,745 DEBUG [https-jsse-nio-443-exec-10] (CallRouting.java:119) - CUCM 172.16.10.102 sends CURRI Keep-Alive
2020-04-15 09:50:04,746 DEBUG [https-jsse-nio-443-exec-8] (CallRouting.java:119) - CUCM 172.16.10.102 sends CURRI Keep-Alive
```

Figure 72: NFContacts – Verify Keep-Alive Messages

Most common issues are:

- Certificates are not trusted. Use a pcap to trace the TLS handshake, you can see which communication side is rejecting the TLS communication.
- Wrong formatted CURRI URL in CUCM configuration, make sure that you have to include the port (443 or 8443) into the URL!

8.1.2 UPDATE TRANSLATION PATTERN

To enable the use of our previously created External Call Control Profile (ECCP), you have to assign it on a translation pattern.

You should select a translation pattern, that is used for all calls that enter the cluster. This will allow NFContacts to try a name resolution of the calling number. Make sure that e164 numbering scheme is used to resolve the contacts.

See a sample configuration below:

Translation Pattern Configuration

Save

Status
Status: Ready

Pattern Definition

Translation Pattern: \+4940555XXXX

Partition: PA_Phones

Description: Inbound Translation

Numbering Plan: < None >

Route Filter: < None >

MLPP Precedence*: Default

Resource Priority Namespace Network Domain: < None >

Route Class*: Default

Calling Search Space: < None >

☐ Use Originator's Calling Search Space

External Call Control Profile: **NF-Contacts**

Route Option:
☒ Route this pattern
☐ Block this pattern: No Error

☐ Provide Outside Dial Tone

☒ Urgent Priority

☒ Do Not Wait For Interdigit Timeout On Subsequent Hops

☐ Route Next Hop By Calling Party Number

☐ Is an Emergency Services Number (used by Emergency Call Handler)

Figure 73: NFContacts – Update Translation Pattern

8.2 NFCONTACTS CONFIGURATION

The configuration of NFContacts is done via a few configuration items.

The available configuration parameters are explained below:

Parameter	Description
Exchange Settings:	
Exchange Enabled	Activates the Sync function for MS Exchange Contact Sync.
Exchange Address	Specifies the host, that is providing the OWA URL. E.g. ,if the OWA URL is https://1.exchange.1and1.eu/owa you should just enter 1.exchange.1and1.eu
Exchange uses HTTPS	Distinguish between HTTPS or HTTP
Automatic Auth With Jabber Credentials	You can enable an automatic authentication by jabber credentials. However this is only applicable, if jabber user ID and OWA login User ID are identical. Furthermore please note that users might not want to sync their contacts, so please check data privacy policies.
LDAP/AD Settings:	
LDAP Enabled	Enables the LDAP source.

LDAP Name	This is a Identifier for you. It is also used within NFAttendant Directory.
LDAP Server IP:	The IP address of the LDAP server, which should act as the source.
LDAP Port	Typical Port 389.
LDAP Search Base	This is the path in the ldap which is root to search recursively. e.g. OU=users,OU=lab,DC=netfarmers,DC=net
LDAP Manager DN	This is the path to the ldap user for authentication purposes. E.g. CN=Appfield-Lab LDAP,CN=Users,DC=netfarmers,DC=net
LDAP Password	The corresponding password of the LDAP Manager DN user.
LDAP Custom Filter	If required, you are able to specify a ldap filter, e.g. objectclass=*
Other LDAP Attributs	There are many fields that can be synced. You have to fill our every field that should be included into the synchronization process, don't leave them blank if you need them. Make sure that Upper Lower Case matches the LDAP Attribut.
CSV Settings:	
CSV Enabled	Enables the CSV source.
CSV Name	This is a Identifier for you. It is also used within NFAttendant Directory.
SMB Path	The path to the SMB share, e.g. smb://10.1.1.41/NFContacts/
Username	The name of the user, if this is a domain user you should include the domain to authentication to work, e.g. appfield-lab-user@netfarmers.net
Password	The corresponding password of the user.
Filename	The Name of the CSV file, which should be synced, e.g. NFContacts-DummyContacts.csv You'll find a sample CSV File in the next chapter.
Resolve Order	
<p>When using multiple sources you have to specify the priority of name resolution. E.g. a match in personal contacts (EXCHANGE) has higher priority then LDAP contacts (LDAP) or CSV contacts (CSV).</p> <p>Then you should configure the order:</p> <p>EXCHANGE</p> <p>LDAP</p> <p>CSV</p>	

Phone Number Normalization	
Normalize Phone Numbers	If enabled, NFContacts will try to modify the received calling number from CUCM in ECCP request and normalize the number to e164 format, according the specified settings.
International Left Hand Zeros	Used to identify an international call, by e.g. 3 leading zero's.
National Left Hand Zeros	Used to identify a national call, by e.g. 2 leading zero's.
Country Code	Used to identify the country code of the calling number for incoming national calls.
Alerting Name Template	Specifies the name resolution format on the phone. You can use variables to create your output template. E.g. #LastName#, #FirstName# - #Company# will result into: Brink, Torsten - Netfarmers
wsExternalReachable	Specifies if the Webservice should be externally reachable.
wsEnabled	Enables/Disables NFContacts globally.

8.2.1 SAMPLE CSV FILE

The following is an example CSV File for your reference:

```
firstName;lastName;company;phoneNumberWork;phoneNumberHome;mobile;mobile2
Torsten;Brink;Damovo;+4967318999414;;+4915161331077;
Sabine;Schmidt;Cisco Systems;+498955555;;;
```

9 OS UPGRADES

The Appfield Appliance provides two ways to upgrade the operating systems and core components of the system:

- Fresh Installation with Restore using OVA.
- OS-Upgrade via CLI using IMG.

Both options are explained in the chapters below. Please note, that NFApp upgrades can be done using the web interface. Please refer to chapter 1.3.1 for further details.

Note:

If you download the backup from the active production server and upload it into the new server, the config will not appear if the server has no valid license.

9.1 FRESH INSTALL

This chapter explains on how to upgrade to a new Appfield Appliance by using the fresh install option. If you're still using a Appfield Appliance in Version 1.x, you **must** use this option.

We do recommend installing the server with a different IP upfront and change the IP later in the maintenance hours.

9.1.1 PREPARATION

1. Note down services running on the AppField and download the latest version.
2. Download the latest AppField OVA.
3. In case NFCallList is used, make sure you are aware of the user 'cdradmin' to restore this password accordingly.

If you do not know the password anymore. Delete the CDR Integration in CUCM (CDR Management) before you start the migration. Otherwise, the cdradmin will be locked in AppField Appliance for 30 minutes after the last wrong login. A restart does not help to shorten up the blocking time.

9.1.2 SETUP THE NEW SERVER

1. Deploy the new OVA
2. Start the VM and login via SSH (admin/admin)

3. Configure IP, Hostname, Domain, DNS, NTP * In case of invalid DNS-settings the changes take up to **5 minutes**. Please press enter during the waiting time otherwise the SSH session gets terminated.
4. Upload the AppField services to the new server
5. Request 2 licenses via support@netfarmers.net
 - a. Temp License with the temp IP
 - b. Final License with new MAC and old IP
6. Upload the temp license
7. Download a Backup from the production server
 - a. The backup should be pulled just before the migration in case NFCallList is implemented in order not to lose too many entries in the users call list.
8. Upload the restore into the new server (if you upload the restore without a license, it will not work)
9. Restart Tomcat
10. Delete logs
11. Optional
 - a. Change cdruser and appupp user password via CLI
 - b. Change SNMP Settings via CLI

The CLI admin and the Web GUI admin is the same user. However, if you restore the server, you are also recovering the admin password but here just the Web GUI password is recovered. Use the password reset in the GUI and reset the password again to also sync the CLI password.

Note:

When running Appfield in HA, you must create the HA Cluster during this procedure. However, as the virtual (HA) IP address is unchangeable we recommend to use a stub (dead end) network for parallel installation and for migration just set the new network in VMWare network configuration.

9.1.3 IN MAINTENANCE WINDOW

1. Shutdown the old production VM.
2. Change the IP of the new server (server will reload)
3. Upload the new license and restart tomcat.
4. The server should run without errors.
5. The NFChefSek phones will need a restart for the feature to work.
6. Check deployed NFApps for correct functionality.

9.2 OS UPGRADE VIA CLI

This chapter explains on how to upgrade to a new Appfield Appliance by using the OS upgrade option. If you're still using a Appfield Appliance in Version 1.x, you can't use this option and have to use the fresh install option.

Note:

We do recommend performing the changes below in a maintenance window. Also make sure to create a VMWare snapshot of the Appfield Appliance to provide an easy and secure fallback to the previous version.

9.2.1 PREPARATION

1. Download the latest AppField IMG.
2. Upload the IMG file using the appupp user via WinSCP to Appfield appliance. Make sure to upload the file in the /upgrade/ folder and that no other .img file exists in this folder. Do not modify or rename the downloaded .img file.

9.2.2 UPGRADE TO INACTIVE PARTITION

1. Login via SSH (admin/admin)
2. Enable logging in your putty terminal (or other client) and log all output into a file. This file may later be useful in case upgrade fails.
3. In Main Menu select option "Patch & OS Upgrade Menu". You'll now see an overview of active and inactive Appfield Appliance versions.
4. Select the option to "Upgrade Appfield OS Version". The installation will try to detect the upgrade file uploaded before and show the filename.
5. If this is the correct file, you can select "START UPGRADE" and confirm your selection. Be aware that the upgrade process will stop services and therefore upgrade is recommended in maintenance window.
6. Upgrade process will now proceed. If you inspect a "missing" status during the process, this is just an informational notice and will not harm upgrade success.
7. When completed successfully look for the message "Upgrade on inactive Partition finished successfully". Upgrade is not completed and you'll be transferred back to the menu.

The upgrade process will restore all required data, like NFApps, Configuration, users & credentials, certificates, etc. from the point of time where the upgrade happened. So you should proceed to the "switch partition" step as soon as possible.

For Appfield HA Cluster installations please perform upgrade on primary node first and then on secondary node before proceeding to the “switch partition” step.

9.2.3 SWITCH PARTITION

1. Login via SSH (admin/admin)
2. Enable logging in your putty terminal (or other client) and log all output into a file. This file may later be useful in case switch fails.
3. In Main Menu select option “Patch & OS Upgrade Menu”. You’ll now see an overview of active and inactive Appfield Appliance versions. Now you should see the upgraded version in the Inactive Partition section.
4. Select the option to “Switch Appfield OS Version and confirm your selection to start the switch version process. Be aware that the switch version process will restart Appfield Appliance and therefore it is recommended to do so in maintenance window.
5. Wait for Appfield Appliance to restart and web interface to be available again.
6. Check, if the version in Appfield web interface is now the upgraded version.

For Appfield HA Cluster installations please perform switch step on primary node first and then on secondary node.