

# NCP Secure Enterprise Client (iOS)

## Release Notes



**Service Release:** 1.1.2.0 r36988  
**Date:** September 2017

### Prerequisites

The following NCP software components are required for the NCP Secure Enterprise Client on a device with iOS 9.3 or later:

- NCP Secure Enterprise VPN Server Version 11.00
- NCP Secure Enterprise Management Server Version 4.05
- NCP Management Console Version 4.05
- NCP Management Plug-in Client Configuration Version 11.00
- NCP Management Plug-in License Management Version 11.00
- NCP Management Plug-in PKI Enrollment Version 4.05
- NCP Management Plug-in Server Configuration Version 11.00

High availability services are optionally available with:

- NCP Secure Enterprise HA Server Version 10.01

### iOS Client Restrictions

The iOS beta client (version 1.0.1) is not compatible with version 1.1.x and must be removed first.

MD5 certificates cannot be used for iOS.

The option "Use fingerprint sensor to connect" cannot be used if "Automatic (VPN On Demand)" is enabled.

## 1. New Features and Enhancements

None

## 2. Improvements / Problems Resolved

Compatibility issues fixed with iOS 11

## 3. Known Issues

None

Next Generation Network Access Technology

# NCP Secure Enterprise Client (iOS)

## Release Notes



**Service Release:** 1.1.1.1 r36390

**Date:** July 2017

### Prerequisites

The following NCP software components are required for the NCP Secure Enterprise Client on a device with iOS 9.3 or later:

- NCP Secure Enterprise VPN Server Version 11.00
- NCP Secure Enterprise Management Server Version 4.05
- NCP Management Console Version 4.05
- NCP Management Plug-in Client Configuration Version 11.00
- NCP Management Plug-in License Management Version 11.00
- NCP Management Plug-in PKI Enrollment Version 4.05
- NCP Management Plug-in Server Configuration Version 11.00

High availability services are optionally available with:

- NCP Secure Enterprise HA Server Version 10.01

### iOS Client Restrictions

The iOS beta client (version 1.0.1) is not compatible with version 1.1.1 and must be removed first.

MD5 certificates cannot be used for iOS.

The option "Use fingerprint sensor to connect" cannot be used if "Automatic (VPN On Demand)" is enabled.

## 1. New Features and Enhancements

None

## 2. Improvements / Problems Resolved

### Hostname

The name which is automatically generated when starting the device is displayed in the Client Info Center under "Hostname" and can be changed in the iOS settings. Secure Enterprise Management can use this "Hostname" to authenticate configuration updates.

Next Generation Network Access Technology

# NCP Secure Enterprise Client (iOS)

## Release Notes



### Crashes on iOS 9.3

Touching the info icon on the client GUI caused devices with iOS 9.3 to crash. This issue has now been resolved.

## 3. Known Issues

None

## 4. Getting Help for the NCP Secure Enterprise Client (iOS)

To ensure that you always have the latest information about NCP's products, always check the NCP website at:

<http://www.ncp-e.com/en/downloads/software/version-information.html>

For further information about the Enterprise Client, visit:

<http://www.ncp-e.com/en/products/centrally-managed-vpn-solution/managed-vpn-client-suite.html>

For further assistance with the NCP Secure Enterprise Client (Win32/64), visit:

<http://www.ncp-e.com/en/company/contact.html>



## 5. Features

### Operating Systems

See Prerequisites on page 1.

### Central Management

Assignment of VPN configuration and certificates via NCP's Secure Enterprise Management

### High Availability Services

Optional for load sharing are NCP's High Availability Services

### Virtual Private Networking

IPsec (Layer 3 Tunneling), RFC conformant;

Event log;

Communication only in the tunnel or Split Tunneling;

DPD;

Network Address Translation Traversal (NAT-T);

IPsec Tunnel Mode;

### Encryption and Encryption Algorithms

*Symmetrical:*

AES-CBC 128, 192, 256 bits;

AES-CTR 128, 192, 256 bits;

AES-GCM 128, 256 bits (only IKEv2);

Blowfish 128, 448 bits;

Triple-DES 112, 168 bits;

SEED;

*Dynamic Process for Key Exchange:*

RSA to 4096 bits;

ECDSA to 521 bits, Seamless Rekeying (PFS);

Hash Algorithms: SHA, SHA-256, SHA-384, SHA-512, MD5, DH-Gruppe 1, 2, 5, 14-18, 19-21, 25, 26;

### Key Exchange Methods

*IKEv1 (Aggressive and Main Mode):*

Pre-shared Key, RSA, XAUTH;

# NCP Secure Enterprise Client (iOS)

## Release Notes



### *IKEv2:*

Pre-shared Key, RSA, EAP-MS CHAPv2, EAP-MD5, EAP-TLS, EAP-PAP, Signature Authentication (RFC 7427), IKEv2 Fragmentation (RFC 7383);

### Strong Authentication

iOS Keychain for using User (soft) Certificates;  
Touch ID;

### VPN Pathfinder

NCP VPN Path Finder Technology, Fallback to HTTPS (Port 443) from IPsec if neither port 500 nor UDP encapsulation are available;

### IP Address Assignment

DHCP;  
IKE Config Mode (IKEv1);  
Config Payload (IKEv2);

### Line Management

DPD with configurable time interval;  
Timeout;  
„VPN on Demand“ for den automatischen Aufbau des VPN-Tunnels und die ausschließliche Kommunikation darüber;

### Data Compression

Deflate

### Other Features

UDP Encapsulation

### Internet Society RFCs and Drafts

RFC 4301 (IPsec), RFC 4303 ESP, RFC 3947 (NAT-T negotiations), RFC 3948 (UDP encapsulation), IKEv1, RFC 3526, ISAKMP, RFC 7296 (IKEv2), RFC 4555 (MOBIKE), RFC 5685 (Redirect), RFC 7383 (Fragmentation), RFC 7427 , 3279 Section 2.2.3, 3447 Section 8 (Signature Authentication), RFC 5903, 6954, 6989, 4754 (ECC), RFC 2451, 3686 (AES with ESP), 5930 (AES-CTR), 4106 (AES-GCM), 5282, 6379 (Suite B), RFC 3447 Section 8 (Padding)

### Client GUI

Intuitive GUI with German and English;

Next Generation Network Access Technology

# NCP Secure Enterprise Client (iOS)

## Release Notes



Configuration Update;  
Profile Selection;  
Connection Control and Management;  
Connection Statistics, Log Files;  
Trace Tool for Error Diagnosis;  
3D Touch;

Next Generation Network Access Technology