NCP Secure Enterprise Client (iOS)
Release Notes

Service Release: **1.2.1.1 r 43310**
Datum: **März 2019**

Voraussetzungen

Folgende NCP Software-Komponenten werden für den Rollout und den Einsatz des NCP Secure Enterprise Clients auf einem Gerät mit iOS 11.x oder neuer benötigt:

- 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 11.14 r42540
- NCP Management Plug-in License Management Version 11.13 r41357
- NCP Management Plug-in PKI Enrollment Version 4.05
- NCP Management Plug-in Server Configuration Version 11.00

Optional stehen die High Availability Services zur Verfügung mit:

- NCP Secure Enterprise HA Server Version 10.01

Hinweise zu Einschränkungen bei Einsatz des iOS Clients

Unter dem Betriebssystem iOS können keine Zertifikate mit dem MD5-Signaturalgorithmus verwendet werden.

Die Option „Benutze Fingerabdrucksensor bei Verbindungsaufbau“ kann nicht verwendet werden, wenn für den Verbindungsaufbau „Automatisch (VPN on demand)“ konfiguriert wurde.

1. Neue Leistungsmerkmale und Erweiterungen

VPN Verbindungsaufbau über Systemeinstellungen

Beim VPN Verbindungsaufbau über die iOS Systemeinstellungen können jetzt auch Profile verwendet werden, die die optionale Eingabe von Benutzername und Passwort (Authentisierung via XAUTH oder EAP) konfiguriert haben.
In diesem Fall wird eine iOS Mitteilung angezeigt, über die in den Client-Monitor gewechselt werden kann, um die Eingabe durchzuführen.

2. Verbesserungen / Fehlerbehebungen

Diverse Optimierungen

3. Bekannte Einschränkungen

Keine

Deutschland: NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Fon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com

Service Release: **1.2.0.0 r42534**
Datum: **Januar 2019**

Voraussetzungen

Folgende NCP Software-Komponenten werden für den Rollout und den Einsatz des NCP Secure Enterprise Clients auf einem Gerät mit iOS 11.x oder neuer benötigt:

- 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 11.14 r42540
- NCP Management Plug-in License Management Version 11.13 r41357
- NCP Management Plug-in PKI Enrollment Version 4.05
- NCP Management Plug-in Server Configuration Version 11.00

Optional stehen die High Availability Services zur Verfügung mit:

- NCP Secure Enterprise HA Server Version 10.01

Hinweise zu Einschränkungen bei Einsatz des iOS Clients

Unter dem Betriebssystem iOS können keine Zertifikate mit dem MD5-Signaturalgorithmus verwendet werden.

Die Option „Benutze Fingerabdrucksensor bei Verbindungsaufbau“ kann nicht verwendet werden, wenn für den Verbindungsaufbau „Automatisch (VPN on demand)“ konfiguriert wurde.

1. Neue Leistungsmerkmale und Erweiterungen

Optionale Abfrage von Benutzername / Passwort vor VPN-Verbindungsaufbau

Optionale Eingabe von Benutzername und Passwort vor dem VPN-Verbindungsaufbau (Authentisierung via XAUTH oder EAP).

2. Verbesserungen / Fehlerbehebungen

Diverse Optimierungen

3. Bekannte Einschränkungen

Keine

Service Release: **1.1.4.1 r41011**
Datum: **September 2018**

Voraussetzungen

Folgende NCP Software-Komponenten werden für den Rollout und den Einsatz des NCP Secure Enterprise Clients auf einem Gerät mit iOS 9.3 oder neuer benötigt:

- 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

Optional stehen die High Availability Services zur Verfügung mit:

- NCP Secure Enterprise HA Server Version 10.01

Hinweise zu Einschränkungen bei Einsatz des iOS Clients

Unter dem Betriebssystem iOS können keine Zertifikate mit dem MD5-Signaturalgorithmus verwendet werden.

Die Option „Benutze Fingerabdrucksensor bei Verbindungsaufbau“ kann nicht verwendet werden, wenn für den Verbindungsaufbau „Automatisch (VPN on demand)“ konfiguriert wurde.

1. Neue Leistungsmerkmale und Erweiterungen

Keine

2. Verbesserungen / Fehlerbehebungen

Anpassungen an das iPhone X

GUI-Anpassungen in der App sowie Anpassungen an Face ID.

Fehlerbehebung in der Online-Hilfe

3. Bekannte Einschränkungen

Keine

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

Voraussetzungen

Folgende NCP Software-Komponenten werden für den Rollout und den Einsatz des NCP Secure Enterprise Clients auf einem Gerät mit iOS 9.3 oder neuer benötigt:

- 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

Optional stehen die High Availability Services zur Verfügung mit:

- NCP Secure Enterprise HA Server Version 10.01

Hinweise zu Einschränkungen bei Einsatz des iOS Clients

Vor Verwendung des iOS Clients der Version 1.1.x muss aufgrund von Inkompatibilitäten der iOS BETA Client (Version 1.0.1) deinstalliert werden.

Unter dem Betriebssystem iOS können keine Zertifikate mit dem MD5-Signaturalgorithmus verwendet werden.

Die Option „Benutze Fingerabdrucksensor bei Verbindungsaufbau“ kann nicht verwendet werden, wenn für den Verbindungsaufbau „Automatisch (VPN on demand)“ konfiguriert wurde.

1. Neue Leistungsmerkmale und Erweiterungen

Keine

2. Verbesserungen / Fehlerbehebungen

Kompatibilitätsprobleme mit iOS 11 behoben

3. Bekannte Einschränkungen

Keine

Service Release: **1.1.1.1 r36390**
Datum: **Juli 2017**

Voraussetzungen

Folgende NCP Software-Komponenten werden für den Rollout und den Einsatz des NCP Secure Enterprise Clients auf einem Gerät mit iOS 9.3 oder neuer benötigt:

- 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

Optional stehen die High Availability Services zur Verfügung mit:

- NCP Secure Enterprise HA Server Version 10.01

Hinweise zu Einschränkungen bei Einsatz des iOS Clients

Vor Verwendung des iOS Clients der Version 1.1.1 muss aufgrund von Inkompatibilitäten der iOS BETA Client (Version 1.0.1) deinstalliert werden.

Unter dem Betriebssystem iOS können keine Zertifikate mit dem MD5-Signaturalgorithmus verwendet werden.

Die Option „Benutze Fingerabdrucksensor bei Verbindungsaufbau“ kann nicht verwendet werden, wenn für den Verbindungsaufbau „Automatisch (VPN on demand)“ konfiguriert wurde.

1. Neue Leistungsmerkmale und Erweiterungen

Keine

2. Verbesserungen / Fehlerbehebungen

Hostname

Der bei Inbetriebnahme des Geräts automatisch generierte „Name“ wird im Client Info Center als „Hostname“ angezeigt und kann über die „Systemeinstellungen“ des iOS-Geräts geändert werden. Der „Hostname“ kann vom Secure Enterprise Management (SEM) zur Authentisierung bei Konfigurations-Updates verwendet werden.

Absturz auf Geräten unter iOS 9.3

Eine Berührung des Infosymbols auf der Client GUI führte auf Geräten mit iOS 9.3 zu einem Absturz. Dieser Fehler ist nun behoben.

3. Bekannte Einschränkungen

Keine

4. Hinweise zum NCP Secure Enterprise Client (iOS)

Weitere Informationen zum letzten Stand der Entwicklung der NCP-Produkte erhalten Sie auf der Website:

http://www.ncp-e.com/de/downloads/download-vpn-client/versionsinformationen.html

Weitere Informationen zum NCP Secure Enterprise Client (Win32/64) finden Sie hier:

http://www.ncp-e.com/de/produkte/zentral-gemanagte-vpn-loesung/managed-vpn-client-suite.html

Weitere Unterstützung bei Fragen zum Enterprise Client, erhalten Sie über die Mail-Adressen auf folgender Seite:

http://www.ncp-e.com/de/unternehmen/kontakt.html

5. Leistungsmerkmale

Betriebssysteme

Beachten Sie dazu die “Voraussetzungen” auf Seite 1.

Zentrales Management

Verteilung der VPN-Konfiguration und Zertifikate über das NCP Secure Enterprise Management

High Availability Services

Optional stehen die High Availability Services zur Verfügung

Virtual Private Networking

IPsec (Layer 3 Tunneling), RFC-konform;
Event log;
Kommunikation nur im Tunnel oder Split Tunneling;
DPD;
NAT-Traversal (NAT-T);
IPsec Tunnel Mode;

Verschlüsselung / Encryption

Symmetrische Verfahren:
AES-CBC 128, 192, 256 Bit;
AES-CTR 128, 192, 256 Bit;
AES-GCM 128, 256 Bit (nur IKEv2);
Blowfish 128, 448 Bit;
Triple-DES 112, 168 Bit;
SEED;
Dynamische Verfahren für den Schlüsselaustausch:
RSA bis 4096 Bit;
ECDSA bis 521 Bit, Seamless Rekeying (PFS);
Hash Algorithmen: SHA, SHA-256, SHA-384, SHA-512, MD5, DH-Gruppe 1, 2, 5, 14-18, 19-21, 25, 26;

Schlüsselaustauschverfahren

IKEv1 (Aggressive und Main Mode):
Pre-shared Key, RSA, XAUTH;
IKEv2:
Pre-shared Key, RSA, EAP-MS CHAPv2, EAP-MD5, EAP-TLS, EAP-PAP,
Signature Authentication (RFC 7427), IKEv2 Fragmentation (RFC 7383);

Starke Authentisierung

iOS Schlüsselbund zur Nutzung von Benutzerzertifikaten;
Touch ID;

VPN Pathfinder

NCP VPN Path Finder Technology, Fallback IPsec / HTTPS (Port 443) wenn Port 500 bzw. UDP Encapsulation nicht möglich ist;

IP Adress-Zuweisung

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

Line Management

DPD mit konfigurierbarem Zeitintervall;
Timeout;
„VPN on Demand“ für den automatischen Aufbau des VPN-Tunnels und die ausschließliche Kommunikation darüber;

Datenkompression

Deflate

Weitere Features

UDP Encapsulation

Internet Society RFCs und 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 Benutzeroberfläche in Deutsch und Englisch;
Konfigurations-Update;
Profilauswahl;
Verbindungssteuerung und –überwachung;
Verbindungsstatistik, Log-Files;
Fehlerdiagnose-Export;
Netzwerkinformationen;
3D Touch;

Deutschland: NCP engineering GmbH · Dombühler Str. 2 · 90449 Nürnberg · Fon +49 911 9968-0 · Fax +49 911 9968-299
Americas: NCP engineering, Inc. · 1045 Linda Vista Ave. Unit-A · Mountain View, CA 94043 · Phone: +1 (650) 316-6273 · www.ncp-e.com