Host Access for the Cloud Web Client

3.1.1

Table of contents

Willkommen beim Host Access for the Cloud-Webclient

Der Rocket® Host Access for the Cloud-Webclient bietet einen browserbasierten HTML5-Zugriff auf 3270-, 5250-, VT-, UTS-, ALC- und T27-Hostanwendungen. Host Access for the Cloud erfordert keine Änderungen an Ihren Desktops: Sie müssen weder Software bereitstellen noch Patches anwenden oder Konfigurationen durchführen. Sie können Benutzern plattformunabhängigen Zugriff auf alle Hostanwendungen gewähren.

Verbindungseinstellungen

Verbindungseinstellungen

Es gibt allgemeine Verbindungseinstellungen, die für alle Hosttypen gelten.

Allgemeine Verbindungseinstellungen

Außerdem gibt es zusätzliche Einstellungen, die spezifisch für Ihren Hosttyp sind.

Einstellungen für 3270 und 5250

T27

UTS

VT

ALC

Allgemeine Verbindungseinstellungen

Diese Optionen gelten für alle unterstützten Hosttypen.

- **Beim Start verbinden**

  Sitzungen sind standardmäßig so konfiguriert, dass sie beim Erstellen oder Öffnen einer Sitzung automatisch eine Verbindung zum Host herstellen. Sie können jedoch auch eine Sitzung einrichten, die nicht automatisch eine Verbindung zum Host aufbaut. Wählen Sie „NEIN“, um eine manuelle Verbindung zum Host herzustellen.

- **Erneut verbinden, wenn der Host die Verbindung beendet**

  Wenn diese Option aktiviert ist, versucht Host Access for the Cloud eine neue Verbindung herzustellen, sobald die Hostverbindung beendet wird.

- **Protokoll**

  Wählen Sie aus der Dropdownliste das Protokoll aus, das für die Kommunikation mit dem Host verwendet werden soll. Um eine Hostverbindung herzustellen, müssen der Webclient und der Hostcomputer dasselbe Netzwerkprotokoll verwenden. Die verfügbaren Werte hängen von dem Host ab, mit dem Sie eine Verbindung herstellen. Dazu gehören:

Protokoll	Beschreibung

TN3270	TN3270 ist eine Form des Telnet-Protokolls. Dieses Protokoll definiert eine bestimmte Anzahl von Spezifikationen für die allgemeine Kommunikation zwischen Desktopcomputern und Hostsystemen. Es verwendet TCP/IP als Transportprotokoll zwischen Desktopcomputern und IBM-Mainframes.
TN3270E	TN3270E oder Telnet Erweitert ist für Benutzer von TCP/IP gedacht, die über ein Telnet-Gateway mit RFC 1647-Implementierung eine Verbindung zum IBM-Mainframe herstellen. Mit dem Protokoll TN3270E können Sie den Verbindungsgerätenamen (auch LU-Name genannt) angeben. Ferner verfügen Sie über Standardunterstützung für die Tasten ATTN und SYSREQ sowie die SNA-Antwortbehandlung. Wenn Sie mit Telnet Erweitert eine Verbindung zu einem Gateway aufbauen, das dieses Protokoll nicht unterstützt, wird stattdessen das Standardprotokoll TN3270 verwendet.
TN5250	TN5250 ist eine Form des Telnet-Protokolls. Dieses Protokoll definiert eine bestimmte Anzahl von Spezifikationen für die allgemeine Kommunikation zwischen Desktopcomputern und Hostsystemen. Es verwendet TCP/IP als Transportprotokoll zwischen Desktopcomputern und AS/400-Computern.
Secure Shell (VT)	Das Konfigurieren von SSH-Verbindungen empfiehlt sich zum Gewährleisten einer sicheren, verschlüsselten Kommunikation zwischen Ihrem Computer und einem zuverlässigen VT-Host über ein unsicheres Netzwerk. Mit SSH-Verbindungen wird neben der Authentifizierung von Clientbenutzer und Hostcomputer auch die Verschlüsselung aller Daten sichergestellt. Zwei Authentifizierungsoptionen stehen zur Verfügung: **Interaktiv über die Tastatur** – Sie können diese Authentifizierungsmethode zum Implementieren verschiedener Arten von Authentifizierungsmechanismen verwenden. Jede aktuell unterstützte Authentifizierungsmethode, die nur die Eingabe des Benutzers erfordert, kann über „Interaktiv über die Tastatur“ ausgeführt werden. **Passwort** – Mit dieser Option wird der Client zur Eingabe eines Passworts für den Host aufgefordert, nachdem eine Verbindung mit dem Host hergestellt wurde. Das Passwort wird dann durch den verschlüsselten Kanal an den Host weitergeleitet.
Telnet (VT)	Telnet ist ein Protokoll aus dem TCP/IP-Paket offener Protokolle. Als Zeichenstromprotokoll überträgt Telnet Benutzereingaben aus Zeichenmodus-Anwendungen zeichenweise über das Netzwerk an den Host, wo sie verarbeitet und als Echorückmeldungen über das Netz gesendet werden.
INT1 (UTS)	Ermöglicht den Zugriff auf Unisys 1100/1200-Hosts über das TCP/IP-Netzwerkprotokoll.

TCPA (T27)	Verwenden Sie dieses Protokoll für die Verbindung mit Hosts der Unisys ClearPath NX/LX Series oder der A Series. Bei der TCPA-Authentifizierung werden die Benutzeranmeldeinformationen überprüft. Bei der richtigen Konfiguration können Sie Sicherheitsanmeldeinformationen vom Anmeldeinformationsserver Ihrer Anwendung anfordern und die Anmeldeinformationen zurück an den Server senden. Wenn der Berechtigungsnachweis gültig ist, wird die Anwendung angemeldet. Sie müssen dann keine Benutzer-ID und kein Passwort eingeben. Wenn der Berechtigungsnachweis jedoch nicht gültig ist, werden Sie zur Eingabe einer Benutzer-ID und eines Passworts aufgefordert.
MATIP (ALC)	Das MATIP-Protokoll (Mapping of Airline Traffic Over Internet Protocol) verwendet TCP/IP für Buchungen, Reservierungen und Airline-spezifischen Datenverkehr.

- **TLS-Sicherheit**

  Über TLS-Protokolle können Clients und Server sichere, verschlüsselte Verbindungen in einem öffentlichen Netzwerk herstellen. Wenn Sie mithilfe von TLS Verbindungen herstellen, authentifiziert Host Access for the Cloud den Server, bevor eine Sitzung geöffnet wird. Alle Daten, die zwischen Host Access for the Cloud und dem Host übertragen werden, werden mit der ausgewählten Verschlüsselungsstufe verschlüsselt.

> **Tipp**
>
> Wenn „TLS-Sicherheit“ auf „TLS 1.3“ oder „TLS 1.2“ festgelegt ist, steht die Option zur Verfügung, den Hostnamen mit dem Namen im Serverzertifikat zu vergleichen. Es wird dringend empfohlen, die Überprüfung des Hostnamens für alle Sitzungen zu aktivieren.

Folgende Optionen stehen zur Auswahl:

Sicherheitsoptionen	Beschreibung
Keine	Es ist keine sichere Verbindung erforderlich.
TLS 1.3	Mit TLS 1.3 verbinden. Wenn **Serveridentität überprüfen** auf **Ja** festgelegt ist, vergleicht der Client den Server- oder Hostnamen mit dem Namen im Serverzertifikat. Es wird dringend empfohlen, die Überprüfung des Hostnamens für alle Sitzungen zu aktivieren.

Sicherheitsoptionen	Beschreibung
TLS 1.2	Mit TLS 1.2 verbinden. Wenn **Serveridentität überprüfen** auf **Ja** festgelegt ist, vergleicht der Client den Server- oder Hostnamen mit dem Namen im Serverzertifikat. Es wird dringend empfohlen, die Überprüfung des Hostnamens für alle Sitzungen zu aktivieren.

- **Emulationsverfolgung aktivieren**

  Sie können festlegen, dass Hostprotokolle für eine Sitzung generiert werden. Die Standardeinstellung ist „Nein“. Wählen Sie „Ja“ aus, damit bei jedem Start der Sitzung eine neue Trace-Datei für den Emulationshost erstellt wird.

Terminal ID Manager verwenden

MSS Um Terminal ID Manager verwenden zu können, muss ein Terminal ID Manager-Server konfiguriert sein. Siehe Terminal ID Manager Guide (Terminal ID Manager-Handbuch).

Terminal ID Manager stellt IDs für Clientanwendungen zur Laufzeit bereit und verwaltet gepoolte IDs für verschiedene Hosttypen. Eine Kennung besteht aus Verbindungsdaten, die für eine einzelne Hostsitzung eindeutig sind.

Wenn Sie Terminal ID Management verwenden möchten und den Terminal ID Management-Server konfiguriert haben, können Sie anhand der nachstehenden Optionen die Kriterien zum Abrufen einer Kennung konfigurieren. Eine Kennung wird nur dann zurückgegeben, wenn alle angegebenen Kriterien erfüllt sind.

> **Hinweis**
>
> Beachten Sie, dass Sie durch Angabe eines Kriteriums festlegen, dass die Kennung nur zugewiesen werden soll, wenn eine Kennung mit dem angegebenen Wert gefunden wurde. Die Kennungsanforderung ist nur erfolgreich, wenn die hier ausgewählte Gruppe von Kriterien genau mit einer Kriteriengruppe übereinstimmt, die für mindestens einen Kennungspool in Terminal ID Management festgelegt wurde.

Kriterien für Terminal ID Management

Kriterium	Beschreibung
Poolname	Definieren Sie dieses Attribut und geben Sie den Namen des Pools ein, um die Kennungssuche auf einen Pool einzugrenzen.
Client-IP-Adresse	Die IP-Adresse des Clientrechners wird in die Anforderung einer Kennung mit einbezogen.
Hostadresse	Die Adresse des für die Sitzung konfigurierten Hosts wird in die Anforderung einer Kennung mit einbezogen.
Hostport	Der Port des für die Sitzung konfigurierten Hosts wird in die Anforderung einer Kennung mit einbezogen.
Name der Sitzung	Wenn Sie diese Option wählen, muss die Kennung für die exklusive Verwendung durch die Sitzung konfiguriert sein.
Sitzungstyp	Der Sitzungstyp (z. B. IBM 3270, IBM 5250, UTS, ALC oder T27) ist immer in Anforderungen für eine Kennung enthalten.
Benutzername	Mit diesem Kriterium können Sie gewährleisten, dass ausschließlich zur exklusiven Verwendung durch bestimmte Benutzer erstellte Kennungen zugewiesen werden. Der Name des aktuellen Benutzers entspricht dem Benutzer, dem die Sitzung zur Laufzeit zugewiesen ist. Der Name muss in einer Kennung gefunden werden, um zugewiesen werden zu können. Für die Konfiguration einer auf Benutzernamen basierenden Sitzung ist ein Standardplatzhalter-Benutzername verfügbar: tidm-setup. Wenn ein Administrator Sitzungen mithilfe von tidm-setup konfigurieren möchte, muss Terminal ID Manager Kennungen für tidm-setup bereitgestellt haben. Sie können den Standardnamen mit einem eigenen Namen überschreiben, indem Sie die Datei `&ltInstallationsverzeichnis>/sessionserver/conf/container.properties` wie folgt ändern: `id.manager.user.name=benutzerdefinierter-Benutzername`. Dabei wird `benutzerdefinierter-Benutzername` durch den Namen ersetzt, den Sie verwenden möchten.

Anwendungsname (UTS)	Der Name der Hostanwendung wird in die Anforderung einer Kennung mit einbezogen.

Um das Verhalten bei der Verbindungsherstellung festzulegen, wenn Terminal ID Management für die betreffende Sitzung keine Kennung zuordnen kann, verwenden Sie **Bei nicht zugeordneter Kennung**:

- **Verbindungsversuch fehlschlagen lassen** – Wenn diese Option aktiviert ist, versucht die Sitzung nicht, eine Verbindung herzustellen, wenn eine Kennung nicht zugeordnet ist.
- **Verbindungsversuch zulassen** – Wenn diese Option aktiviert ist, versucht die Sitzung, eine Verbindung herzustellen, wenn eine Kennung nicht zugeordnet ist. Der Versuch kann jedoch vom Host abgelehnt werden. Bei einigen Hosttypen können Benutzer ohne Kennung eine Verbindung herstellen.

  Klicken Sie auf Terminal ID Manager-Kriterien testen, um zu bestätigen, dass Terminal ID Manager mithilfe der ausgewählten Kriterien und Werte eine Kennung bereitstellen kann.
- **Pakete zum Aktivhalten senden** – Verwenden Sie diese Einstellung, um die Verbindung zwischen Ihrer Sitzung und dem Host kontinuierlich zu überprüfen, sodass eventuelle Verbindungsprobleme zeitnah erkannt werden. Es stehen folgende Typen von Keep-Alive-Paketen zur Auswahl:

Option	Funktion
Keine	Standardeinstellung. Es werden keine Pakete gesendet.
System	Der TCP/IP-Stapel überwacht die Hostverbindung und sendet ab und zu Keep-Alive-Pakete. Bei dieser Option werden weniger Systemressourcen als bei den Optionen „NOP-Pakete senden“ oder „Taktmarkenpakete senden“ verwendet.
NOP-Pakete senden	Ein NOP-Befehl („No Operation“, keine Operation) wird in regelmäßigen Abständen an den Host gesendet. Der Host muss auf diese Befehle nicht antworten; der TCP/IP-Stapel kann jedoch feststellen, ob beim Zustellen des Pakets ein Problem auftritt.
Taktmarkenpakete senden	Ein Taktmarkenbefehl wird in regelmäßigen Abständen an den Host gesendet, um zu prüfen, ob die Verbindung noch aktiv ist. Der Host sollte auf diese Befehle antworten. Wenn keine Antwort eingeht oder beim Senden des Pakets ein Fehler auftritt, wird die Verbindung getrennt.

- **Zeitlimit zum Aktivhalten (Sekunden)** – Wenn Sie die Option „NOP-Pakete senden“ oder „Taktmarkenpakete senden“ auswählen, wählen Sie das Intervall zwischen den

Sendeanforderungen zum Aktivhalten aus. Die Werte liegen zwischen 1 und 36000 Sekunden (eine Stunde); der Standardwert ist 600 Sekunden.

Terminal ID Manager-Kriterien testen

Terminal ID Management gibt zur Laufzeit Kennungen an Clientanwendungen aus. Verwenden Sie diese Testoption, um zu bestätigen, dass Terminal ID Management mithilfe der ausgewählten Kriterien und Werte eine Kennung bereitstellen kann.

Die Kriterien für die aktuelle Sitzung werden im Bereich „Verbindung“ angegeben, nachdem Sie entweder über den Gerätenamen (3270- und 5250-Hosttypen), das Feld „Terminalkennung (UTS)“ oder das Feld „Stationskennung“ (T27) die Option **Terminal ID Management verwenden** ausgewählt haben. Standardmäßig werden die ausgewählten Kriterien für die aktuelle Sitzung angezeigt.

Klicken Sie auf **Testen**, um zu überprüfen, ob Terminal ID Management eine Kennung bereitstellen kann, die mit den konfigurierten und ausgewählten Kriterien und Werten übereinstimmt. Der Test gibt den Namen einer verfügbaren Kennung zurück, die die ausgewählten Attributkriterien erfüllt.

Testen weiterer Kriterien und Werte

In diesem Bereich können Sie Kriterien testen, die sich von denen für die aktuelle Sitzung unterscheiden.

1. Wählen Sie beliebige Einträge aus der Liste „Sitzungstyp“ aus und geben Sie die zu testenden Kriterien an. Sie können alternative Werte testen, die Sie in einer Terminal ID Management-Beispielanfrage verwenden möchten.
2. Klicken Sie auf **Testen**, um zu überprüfen, ob Terminal ID Management eine Kennung bereitstellen kann, die mit den ausgewählten Kriterien und Werten übereinstimmt. Der Test gibt den Namen einer verfügbaren Kennung zurück, die die ausgewählten Werte erfüllt.

3270- und 5250-Verbindungseinstellungen

3270- und 5250-Hosttypen erfordern neben den allgemeinen Verbindungseinstellungen die nachstehenden spezifischen Einstellungen.

- **Terminalmodell**

  Geben Sie das Terminalmodell (die Anzeigestation) an, das von Host Access for the Cloud emuliert werden soll. Je nach Hosttyp sind unterschiedliche Terminalmodelle verfügbar.

Wenn Sie **Benutzerdefiniertes Modell** wählen, können Sie das Terminalmodell durch Festlegen der Anzahl der Spalten und Zeilen anpassen.

- **Automatische Kerberos-Anmeldung verwenden (nur 5250)** MSS

  Wenn dies auf **Ja** festgelegt ist, muss der Benutzer keine Anmeldeberechtigung eingeben. Die automatische Kerberos-Anmeldung wird unter „MSS-Verwaltungskonsole > Host Access for the Cloud“ konfiguriert. In Bezug auf die Konfiguration von HACloud zur Verwendung des Kerberos-Authentifizierungsprotokolls sollten Sie mit bestimmten Begriffen vertraut sein und die zu erfüllenden Voraussetzungen kennen, bevor Sie diese Option konfigurieren. Diese Optionen sind ausführlich in der Dokumentation im Bereich „Host Access for the Cloud“ der MSS-Verwaltungskonsole beschrieben, die über die Hilfe-Schaltfläche verfügbar ist. Weitere Informationen finden Sie im Deployment Guide (Bereitstellungshandbuch).

- **Terminalkennung** (nur 3270)

  Wenn Host Access for the Cloud eine Verbindung zu einem Telnet-Host herstellt, handeln das Telnet-Protokoll und der Host eine Terminalkennung aus, die während der anfänglichen Telnet-Verbindung verwendet wird. In der Regel einigen sich beide Seiten bei der Aushandlung auf die richtige Terminalkennung, sodass Sie dieses Feld leer lassen sollten.

- **TLS-Sicherheit**

  Über TLS-Protokolle können Clients und Server sichere, verschlüsselte Verbindungen in einem öffentlichen Netzwerk herstellen. Wenn Sie mithilfe von TLS Verbindungen herstellen, authentifiziert Host Access for the Cloud den Server, bevor eine Sitzung geöffnet wird. Alle Daten, die zwischen Host Access for the Cloud und dem Host übertragen werden, werden mit der ausgewählten Verschlüsselungsstufe verschlüsselt. Ausführliche Informationen zu dieser allgemeinen Einstellung finden Sie unter Allgemeine Verbindungseinstellungen.

- **Gerätename**

  Wenn Sie als Protokoll TN3270, TN3270E oder TN5250 ausgewählt haben, geben Sie den Gerätenamen an, der bei der Verbindung der Sitzung zum Host verwendet werden soll. Der Gerätename ist auch unter der Bezeichnung Host-LU oder Pool bekannt. Zudem können Sie folgende Optionen auswählen:

  - **Eindeutigen Gerätenamen generieren** – Generiert automatisch einen eindeutigen Gerätenamen.
  - **Terminal ID Manager verwenden** – Zeigt zusätzliche Einstellungen zum Festlegen an. Siehe Verwenden von Terminal ID Manager.
  - **Benutzer immer zur Eingabe der ID auffordern** – Der Endbenutzer wird bei jedem Verbindungsversuch aufgefordert, die Geräte-ID einzugeben.
  - **Benutzer zur Eingabe auffordern, falls ID nicht angegeben** OBJ – Der Endbenutzer wird beim ersten Verbindungsversuch zur Eingabe aufgefordert und der eingegebene Wert wird gespeichert. Der gespeicherte Wert wird dann ohne weitere Aufforderungen verwendet.