

PCoIP ゼロクライアント/ ホスト管理者ガイド

TER1206003

第1版





Teradici Corporation
#101-4621 Canada Way, Burnaby, BC V5G 4X8 Canada
p +1 604 451 5800 f +1 604 451 5818
www.teradici.com

このドキュメントに含まれる情報は、書類発行日時点における Teradici Corporation の最新の見解を述べています。Teradici は変化する市場動向に対応するので、それを Teradici 側による誓約と解釈すべきではありません。そして Teradici は、書類発行日以降に存在するあらゆる情報の正確性について保証することは出来ません。

このドキュメントは情報の開示を目的とします。TERADICI はこのドキュメントの情報に関して、表現又は暗黙や法律に従う保証を一切行いません。

ユーザには、全ての適切な著作権に従う責任があります。著作権法で定められた権利を制限すること無しに、このドキュメントの複製、盗用あるいは公的システムへの開示、又はあらゆる手段（電子的、機械的、写真、録音その他）による転送は、Teradici Corporation からの書面による許可無しに行う事は出来ません。

Teradici は、このドキュメント中の概念について特許、特許申請、商標、著作権または他の知的財産権を持つ場合があります。Teradici により明白に提供されたいかなるライセンス契約書無くして、このドキュメントの提出が、これらの特許、商標、著作権またはその他の知的財産に関するライセンスを与えることはありません。詳細については、<http://www.teradici.com/teradici/pat.php> を参照してください。

© 2012 Teradici Corporation. All rights reserved.

Teradici、PC-over-IP 及び PCoIP は、Teradici Corporation の登録商標です。

ここに記載される実際の企業および製品名は、それら所有者の商標である場合があります。

目次

図一覧	11
表一覧	15
1 ようこそ	18
イントロダクション	18
2 最新情報	20
ファームウェア 4.0.2 の最新情報	20
3 PCoIP 管理ツール	22
MC について	22
MC へのログイン	23
MC Home ページ	23
MC Profile Management ページ	24
MC Manage Profiles ページ	25
AWI について	29
AWI へのログイン	29
AWI Initial Setup ページ	30
AWI Home ページ	31
AWI メニュー	35
OSD について	36
セッションへの接続	37
セッションの切断	41
オーバーレイウィンドウ	43
Display Link Training Failed	43
Half Duplex オーバーレイ	43
Network Connection Lost オーバーレイ	43
No Support Resolutions Found	44
Preparing Desktop オーバーレイ	44
USB Device Not Authorized オーバーレイ	44
USB Over Current Notice オーバーレイ	45
USB Device Not Supported Behind a High-speed Hub オーバーレイ	45
Resolution Not Supported オーバーレイ	45
Video Source オーバーレイ	46
OSD メニュー	46
4 PCoIP デプロイメントシナリオ	48

PCoIP ホストカードとゼロクライアント	48
プロセッサ情報の表示	49
TERA1100 ゼロクライアントと TERA1202 ホストカードの接続	51
前提条件	52
セッション接続タイプ	53
ホストとクライアントの静的な接続	53
SLP ホストディスカバリを使用したホストとクライアントの接続	54
サードパーティ製コネクションブローカを使用したホストとクライアントの接続	54
VMware View Connection Server ブローカを使用したホストとクライアントの接続	55
その他の設定リンク	55
TERA2321 ゼロクライアントと TERA1202 ホストカードの接続	57
前提条件	58
セッション接続タイプ	59
ホストとクライアントの静的な接続	59
SLP ホストディスカバリを使用したホストとクライアントの接続	60
サードパーティ製コネクションブローカを使用したホストとクライアントの接続	60
VMware View Connection Server ブローカを使用したホストとクライアントの接続	61
その他の設定リンク	61
TERA2140 ゼロクライアントと TERA1202 ホストカードの接続	63
前提条件	64
セッション接続タイプ	65
ホストとクライアントの静的な接続	65
SLP ホストディスカバリを使用したホストとクライアントの接続	66
サードパーティ製コネクションブローカを使用したホストとクライアントの接続	66
VMware View Connection Server ブローカを使用したホストとクライアントの接続	67
その他の設定リンク	67
TERA1100 ゼロクライアントと TERA2220 ホストカードの接続	69
前提条件	70
セッション接続タイプ	71
ホストとクライアントの静的な接続	71
SLP ホストディスカバリを使用したホストとクライアントの接続	72
サードパーティ製コネクションブローカを使用したホストとクライアントの接続	72
VMware View Connection Server ブローカを使用したホストとクライアントの接続	73
その他の設定リンク	73
TERA2321 ゼロクライアントと TERA2220 ホストカードの接続	75
前提条件	76
セッション接続タイプ	77
ホストとクライアントの静的な接続	77
SLP ホストディスカバリを使用したホストとクライアントの接続	78
サードパーティ製コネクションブローカを使用したホストとクライアントの接続	78
VMware View Connection Server ブローカを使用したホストとクライアントの接続	79

その他の設定リンク	79
TERA2140 ゼロクライアントと TERA2220 ホストカードの接続.....	81
前提条件	82
セッション接続タイプ	83
ホストとクライアントの静的な接続	83
SLP ホストディスカバリを使用したホストとクライアントの接続.....	84
サードパーティ製接続ブローカを使用したホストとクライアントの接続.....	84
VMware View Connection Server ブローカを使用したホストとクライアントの接続.....	85
その他の設定リンク	85
TERA1100 ゼロクライアントと TERA2240 ホストカードの接続.....	87
前提条件	88
セッション接続タイプ	89
ホストとクライアントの静的な接続	89
SLP ホストディスカバリを使用したホストとクライアントの接続.....	90
サードパーティ製接続ブローカを使用したホストとクライアントの接続.....	90
VMware View Connection Server ブローカを使用したホストとクライアントの接続.....	91
その他の設定リンク	91
TERA2321 ゼロクライアントと TERA2240 ホストカードの接続.....	93
前提条件	94
セッション接続タイプ	95
ホストとクライアントの静的な接続	95
SLP ホストディスカバリを使用したホストとクライアントの接続.....	96
サードパーティ製接続ブローカを使用したホストとクライアントの接続.....	96
VMware View Connection Server ブローカを使用したホストとクライアントの接続.....	97
その他の設定リンク	97
TERA2140 ゼロクライアントと TERA2240 ホストカードの接続.....	99
前提条件	100
セッション接続タイプ	101
ホストとクライアントの静的な接続	101
SLP ホストディスカバリを使用したホストとクライアントの接続.....	102
サードパーティ製接続ブローカを使用したホストとクライアントの接続.....	102
VMware View Connection Server ブローカを使用したホストとクライアントの接続.....	103
その他の設定リンク	103
TERA1100 ゼロクライアントと VMware View 仮想デスクトップの接続	105
前提条件	106
セッション接続タイプ	107
View Connection Server	107
View Connection Server + 自動ログオン	108
View Connection Server + キオスク	108
View Connection Server + Imprivata OneSign	109
その他の設定リンク	109

	TERA2321 ゼロクライアントと VMware View 仮想デスクトップの接続	111
	前提条件	112
	セッション接続タイプ	112
	View Connection Server	113
	View Connection Server + 自動ログオン	113
	View Connection Server + キオスク	113
	View Connection Server + Imprivata OneSign.....	114
	その他の設定リンク	114
	TERA2140 ゼロクライアントと VMware View 仮想デスクトップの接続	116
	前提条件	117
	セッション接続タイプ	118
	View Connection Server	118
	View Connection Server + 自動ログオン	119
	View Connection Server + キオスク	119
	View Connection Server + Imprivata OneSign.....	120
	その他の設定リンク	120
	VMware View クライアントと VMware View 仮想デスクトップの接続	122
5	PCoIP GUI リファレンス	123
	初期セットアップ	123
	AWI ホスト : Initial Setup ページ.....	123
	AWI クライアント : Initial Setup ページ.....	125
	ネットワークの設定	126
	MC : ネットワーク設定.....	126
	AWI : ネットワーク設定.....	129
	OSD : ネットワーク設定.....	132
	ラベル設定.....	134
	AWI : ラベル設定	134
	OSD : ラベル設定	135
	デバイスディスカバリの設定	137
	MC : ディスカバリ設定.....	137
	AWI : ディスカバリ設定.....	139
	OSD : ディスカバリ設定.....	140
	SNMP の設定.....	141
	MC : SNMP 設定に関するヘルプ	141
	AWI : SNMP 設定	141
	セッションの設定	142
	セッションの設定	142
	MC : Direct to Host セッション設定.....	144
	MC : Direct to Host Session + SLP ホストディスカバリ設定	147
	MC : View Connection Server セッション設定	150

MC : View Connection Server + 自動ログオンセッション設定.....	154
MC : View Connection Server + キオスクセッション設定.....	159
MC : View Connection Server + Imprivata OneSign セッション設定.....	162
MC : Connection Management Interface 設定.....	166
AWI ホスト : Direct from Client セッション設定.....	169
AWI クライアント : Direct to Host セッション設定.....	170
AWI クライアント : Direct to Host + SLP ホストディスカバリセッション設定.....	175
AWI クライアント : View Connection Server セッション設定.....	178
AWI クライアント : View Connection Server + 自動ログオンセッション設定.....	185
AWI クライアント : View Connection Server + キオスクセッション設定.....	191
AWI クライアント : View Connection Server + Imprivata OneSign セッション設定.....	196
AWI ホスト : Connection Management Interface セッション設定.....	201
AWI クライアント : Connection Management Interface セッション設定.....	204
OSD : Direct to Host セッション設定.....	208
OSD : Direct to Host + SLP ホストディスカバリセッション設定.....	211
OSD : View Connection Server セッション設定.....	214
OSD : View Connection Server + 自動ログオンセッション設定.....	217
OSD : View Connection Server + キオスクセッション設定.....	222
OSD : View Connection Server + Imprivata OneSign セッション設定.....	225
OSD : Connection Management Interface セッション設定.....	229
セッション暗号化の設定.....	232
MC : 暗号化設定.....	232
AWI : 暗号化設定に関するヘルプ.....	234
セッション帯域幅の設定.....	234
MC : 帯域幅設定.....	234
AWI : 帯域幅設定.....	236
言語の設定.....	238
MC : 言語設定.....	238
AWI クライアント : 言語設定.....	239
OSD : 言語設定.....	240
OSD パラメータの設定.....	242
MC : OSD 設定.....	242
AWI クライアント : OSD 設定.....	243
OSD : OSD 設定.....	243
イメージ品質の設定.....	244
MC : イメージ設定.....	244
AWI ホスト : イメージ設定.....	247
AWI クライアント : イメージ設定.....	249
OSD : イメージ設定.....	251
モニタエミュレーションの設定.....	253
MC : モニタエミュレーション.....	253
AWI Tera1 ホスト : モニタエミュレーション.....	254

AWI Tera2 ホスト：モニタエミュレーション	255
時間の設定	257
MC：時間設定	257
AWI：時間設定	258
セキュリティの設定	260
MC：セキュリティ設定	260
AWI：セキュリティ設定に関するヘルプ	261
オーディオ承認の設定	261
MC：オーディオ承認	261
AWI Tera1 ホスト：オーディオ承認	263
AWI クライアント：オーディオ承認	264
電源承認の設定	265
MC：電源承認	265
AWI Tera1 クライアント：電源承認	266
ホストドライバ機能の設定	267
MC：ホストドライバ機能	267
AWI ホスト：ホストドライバ機能	268
イベントログの設定	269
MC：イベントログ設定	269
AWI：イベントログ設定	271
OSD：イベントログ設定	274
周辺機器の設定	275
MC：周辺機器設定	275
AWI クライアント：周辺機器設定に関するヘルプ	275
IPv6 の設定	276
MC：IPv6 設定	276
AWI：IPv6 設定	278
OSD：IPv6 設定	280
ディスプレイポロジの設定	281
MC：ディスプレイポロジ設定	281
OSD デュアルディスプレイ：ディスプレイポロジ設定	285
OSD クアッドディスプレイ：ディスプレイポロジ設定	288
OSD ロゴのアップロード	290
MC：OSD ロゴ設定	290
AWI クライアント：OSD ロゴ設定	291
ファームウェアのアップロード	292
MC：ファームウェア管理	292
AWI：ファームウェアアップロード設定	293
USB 承認の設定	295
MC：USB 承認	295
AWI クライアント：USB 承認	298

AWI ホスト：USB 承認	302
証明書ストアの設定	306
MC：証明書ストア管理	306
AWI：証明書アップロード設定	308
OSD ディスプレイオーバーライドの設定	309
OSD デュアルディスプレイ：ディスプレイ設定	309
OSD クラッドディスプレイ：ディスプレイ設定	312
パスワードとリセットパラメータの設定 (AWI/OSD)	314
AWI：パスワード設定	314
OSD：パスワード設定	315
AWI ホスト：パラメータリセット設定	316
AWI クライアント：パラメータリセット設定	317
OSD：パラメータリセット設定	318
診断の表示 (AWI/OSD)	319
AWI：イベントログ設定に関するヘルプ	319
OSD：イベントログ設定に関するヘルプ	319
AWI ホスト：セッション制御設定	320
AWI クライアント：セッション制御設定	321
AWI ホスト：セッション統計情報設定	322
AWI クライアント：セッション統計情報設定	324
OSD：セッション統計情報設定	327
AWI ホスト：ホスト CPU 設定	328
AWI クライアント：オーディオ設定	329
AWI クライアント：ディスプレイ設定	330
AWI：PCoIP プロセッサ設定	331
OSD：PCoIP プロセッサ設定	331
OSD：Ping 設定	332
情報の表示 (AWI/OSD)	333
AWI：バージョン情報	333
バージョン情報の表示	335
AWI ホスト：接続デバイス情報	336
AWI クライアント：接続デバイス情報	337
ユーザ設定の構成 (OSD)	339
OSD：VMware View 証明書チェック設定	339
MC：VMware View 証明書チェック設定に関するヘルプ	340
AWI クライアント：VMware View 証明書チェック設定に関するヘルプ	340
OSD：マウス設定	340
OSD：キーボード設定	341
OSD：イメージ設定に関するヘルプ	342
OSD：ディスプレイトポロジ設定に関するヘルプ	342
OSD：タッチスクリーン設定	343

6	PCoIP テクノロジリファレンス.....	347
	PCoIP ホストカード.....	347
	PCoIP ゼロクライアント.....	347
	DVI インターフェースと DisplayPort インターフェース.....	347
	2560x1600 ディスプレイ解像度のサポート.....	348
	PCoIP コネクションブローカ.....	349
	APEX 2800 PCoIP サーバオフロードカード.....	349
7	用語集（略語、頭字語）.....	351

図一覧

図 3-1 : MC ログインページ.....	23
図 3-2 : MC Home ページ.....	24
図 3-3 : MC Profile Management ページ.....	25
図 3-4 : MC Manage Profiles ページ.....	26
図 3-5 : Edit Properties リンク.....	26
図 3-6 : ネットワーク設定用の Set Properties ページ.....	27
図 3-7 : MC Manage Profiles ページ – 設定後.....	28
図 3-8 : AWI Log In ページ.....	30
図 3-9 : AWI ホスト : Home ページ.....	31
図 3-10 : AWI クライアント : Home ページ.....	32
図 3-11 : AWI メニューの概要.....	36
図 3-12 : OSD メインウィンドウ.....	37
図 3-13 : OSD ホスト方向接続ウィンドウ.....	38
図 3-14 : OSD 接続ステータス.....	38
図 3-15 : OSD View Connection Server 接続ウィンドウ.....	39
図 3-16 : 仮想デスクトップのログインページ.....	39
図 3-17 : OSD View Connection Server 証明書の警告.....	40
図 3-18 : 安全でない警告が表示された OSD ログイン画面.....	40
図 3-19 : OSD VMware View ページ.....	41
図 3-20 : Zero Client Control Panel.....	42
図 3-21 : Display Link Training Failed オーバーレイ.....	43
図 3-22 : Half Duplex オーバーレイ.....	43
図 3-23 : Network Connection Lost オーバーレイ.....	44
図 3-24 : No Support Resolutions Found オーバーレイ.....	44
図 3-25 : Preparing Desktop オーバーレイ.....	44
図 3-26 : USB Device Not Authorized オーバーレイ.....	45
図 3-27 : USB Over Current Notice オーバーレイ.....	45
図 3-28 : USB Device Not Supported Behind a High-speed Hub オーバーレイ.....	45
図 3-29 : Resolution Not Supported オーバーレイ.....	45
図 3-30 : No Source Signal オーバーレイ.....	46
図 3-31 : Source Signal on Other Port オーバーレイ.....	46
図 3-32 : OSD Options メニュー.....	47
図 4-1 : AWI Home ページ上のプロセッサ情報.....	49
図 4-2 : AWI Version ページ上のプロセッサファミリ情報.....	50
図 4-3 : OSD Version ページ上のプロセッサファミリ情報.....	51
図 4-4 : TERA1100 ゼロクライアントと TERA1202 ホストカードの接続.....	52
図 4-5 : TERA2321 ゼロクライアントと TERA1202 ホストカードの接続.....	58
図 4-6 : TERA2140 ゼロクライアントと TERA1202 ホストカードの接続.....	64
図 4-7 : TERA1100 ゼロクライアントと TERA2220 ホストカードの接続.....	70
図 4-8 : TERA2321 ゼロクライアントと TERA2220 ホストカードの接続.....	76
図 4-9 : TERA2140 ゼロクライアントと TERA2220 ホストカードの接続.....	82
図 4-10 : TERA1100 ゼロクライアントと TERA2240 ホストカードの接続.....	88
図 4-11 : TERA2321 ゼロクライアントと TERA2240 ホストカードの接続.....	94
図 4-12 : TERA2140 ゼロクライアントと TERA2240 ホストカードの接続.....	100
図 4-13 : TERA1100 ゼロクライアントと VMware View 仮想デスクトップの接続.....	106

図 4-14 : TERA2321 ゼロクライアントと VMware View 仮想デスクトップの接続	111
図 4-15 : TERA2140 ゼロクライアントと VMware View 仮想デスクトップの接続	117
図 5-1 : AWI ホスト Initial Setup ページ	123
図 5-2 : AWI クライアント Initial Setup ページ	125
図 5-3 : MC ネットワーク設定	127
図 5-4 : AWI Network ページ	129
図 5-5 : OSD Network ページ	132
図 5-6 : AWI Label ページ	135
図 5-7 : OSD Label ページ	136
図 5-8 : MC ディスカバリ設定	138
図 5-9 : AWI Discovery ページ	139
図 5-10 : OSD Discovery ページ	141
図 5-11 : AWI SNMP ページ	142
図 5-12 : MC セッション接続タイプ – Direct to Host	145
図 5-13 : MC セッション接続タイプ – Direct to Host + SLP ホストディスカバリ	148
図 5-14 : MC セッション接続タイプ – View Connection Server	150
図 5-15 : MC セッション接続タイプ – View Connection Server + 自動ログオン	155
図 5-16 : MC セッション接続タイプ – View Connection Server + キオスク	159
図 5-17 : MC セッション接続タイプ – View Connection Server + Imprivata OneSign	163
図 5-18 : MC セッション接続タイプ – Connection Management Interface	167
図 5-19 : AWI セッション接続タイプ – Direct from Client	169
図 5-20 : AWI セッション接続タイプ – Direct to Host	171
図 5-21 : AWI セッション接続タイプ – Direct to Host + SLP ホストディスカバリ	175
図 5-22 : AWI セッション接続タイプ – View Connection Server	179
図 5-23 : Self Help Link オプションの有効化	184
図 5-24 : AWI セッション接続タイプ – View Connection Server + 自動ログオン	185
図 5-25 : Self Help Link オプションの有効化	190
図 5-26 : AWI セッション接続タイプ – View Connection Server + キオスク	192
図 5-27 : AWI セッション接続タイプ – View Connection Server + Imprivata OneSign	197
図 5-28 : AWI セッション接続タイプ – Connection Management Interface (ホスト)	202
図 5-29 : AWI セッション接続タイプ – Connection Management Interface (クライアント)	205
図 5-30 : OSD セッション接続タイプ – Direct to Host	208
図 5-31 : Advanced Settings	209
図 5-32 : OSD セッション接続タイプ – Direct to Host + SLP ホストディスカバリ	211
図 5-33 : Advanced Settings	212
図 5-34 : OSD セッション接続タイプ – View Connection Server	214
図 5-35 : Advanced Settings	215
図 5-36 : OSD セッション接続タイプ – View Connection Server + 自動ログオン	218
図 5-37 : Advanced Settings	219
図 5-38 : OSD セッション接続タイプ – View Connection Server + キオスク	222
図 5-39 : Advanced Settings	223
図 5-40 : OSD セッション接続タイプ – View Connection Server + Imprivata OneSign	226
図 5-41 : Advanced Settings	226
図 5-42 : OSD セッション接続タイプ – Connection Management Interface	230
図 5-43 : Advanced Settings	230
図 5-44 : MC 暗号化設定	233
図 5-45 : MC 帯域幅設定	235
図 5-46 : AWI Bandwidth ページ	237
図 5-47 : MC 言語設定	239

図 5-48 : AWI クライアント Language ページ	240
図 5-49 : OSD Language ページ	241
図 5-50 : MC OSD 設定	242
図 5-51 : AWI On Screen Display ページ	243
図 5-52 : OSD OSD ページ	244
図 5-53 : MC イメージ設定	245
図 5-54 : AWI ホスト Image ページ	247
図 5-55 : AWI ホスト Image ページ – Use Client Image Settings が無効になっている場合	247
図 5-56 : AWI クライアント Image ページ	250
図 5-57 : OSD Image ページ	252
図 5-58 : MC Monitor Emulation ページ	253
図 5-59 : AWI Tera1 ホスト Monitor Emulation ページ	255
図 5-60 : AWI Tera2 ホスト Monitor Emulation ページ	256
図 5-61 : MC 時間設定	257
図 5-62 : AWI Time ページ	259
図 5-63 : MC セキュリティ設定	260
図 5-64 : MC オーディオ承認	262
図 5-65 : AWI Tera1 ホスト Audio ページ	263
図 5-66 : AWI クライアント Audio ページ	264
図 5-67 : MC 電源承認	265
図 5-68 : AWI Tera1 クライアント Power ページ	266
図 5-69 : MC ホストドライバ設定	268
図 5-70 : AWI Host Driver Function ページ	269
図 5-71 : MC イベントログ管理	270
図 5-72 : AWI Event Log ページ	272
図 5-73 : OSD Event Log ページ	274
図 5-74 : MC 周辺機器設定	275
図 5-75 : MC IPv6 設定	276
図 5-76 : AWI IPv6 ページ	278
図 5-77 : OSD IPv6 ページ	280
図 5-78 : MC ディスプレイトポロジ設定	282
図 5-79 : OSD Tera1 Display Topology ページ	286
図 5-80 : OSD Tera2 Display Topology ページ	288
図 5-81 : MC Profile OSD Logo 設定	290
図 5-82 : MC Add OSD Logo 設定	291
図 5-83 : AWI クライアント OSD Logo Upload ページ	291
図 5-84 : MC Profile Firmware 設定	292
図 5-85 : MC Link to Imported Firmware	292
図 5-86 : MC Link to Imported Firmware - 設定後	293
図 5-87 : AWI Firmware Upload ページ	294
図 5-88 : MC プロファイルゼロクライアント USB 設定	295
図 5-89 : USB 許可 – Add New	297
図 5-90 : USB 非許可 – Add New	297
図 5-91 : USB ブリッジ – Add New	297
図 5-92 : AWI クライアント USB ページ	299
図 5-93 : デバイスクラスパラメータ	301
図 5-94 : デバイス ID パラメータ	301
図 5-95 : USB ブリッジパラメータ	302
図 5-96 : AWI ホスト USB ページ	304

図 5-97 : デバイスクラスパラメータ	305
図 5-98 : デバイス ID パラメータ	305
図 5-99 : MC 証明書ストア設定	306
図 5-100 : MC Add Certificate to Store	307
図 5-101 : MC Certificate Store	308
図 5-102 : AWI Certificate Upload ページ	309
図 5-103 : OSD Tera1 Display ページ	310
図 5-104 : OSD Tera2 Display ページ	313
図 5-105 : AWI Password ページ	315
図 5-106 : OSD Change Password ページ	316
図 5-107 : AWI ホスト Reset ページ	317
図 5-108 : AWI クライアント Reset ページ	317
図 5-109 : OSD Reset ページ	319
図 5-110 : AWI ホスト Session Control ページ	320
図 5-111 : AWI クライアント Session Control ページ	321
図 5-112 : AWI ホスト Session Statistics ページ	322
図 5-113 : AWI クライアント Session Statistics ページ	325
図 5-114 : OSD Session Statistics ページ	328
図 5-115 : AWI Host CPU ページ	329
図 5-116 : AWI クライアント Audio ページ	330
図 5-117 : AWI クライアント Display ページ	330
図 5-118 : AWI PCoIP Processor ページ	331
図 5-119 : OSD PCoIP Processor ページ	332
図 5-120 : OSD Ping ページ	333
図 5-121 : AWI Version ページ	334
図 5-122 : OSD Version ページ	335
図 5-123 : AWI ホスト Attached Devices ページ	337
図 5-124 : AWI クライアント Attached Devices ページ	338
図 5-125 : OSD VMware View ページ	339
図 5-126 : OSD Mouse ページ	341
図 5-127 : OSD Keyboard ページ	342
図 5-128 : OSD Touch Screen ページ	343
図 6-1 : 2560x1600 解像度用の DVI コネクタと DisplayPort コネクタ	348

表一覧

表 3-1 : AWI Home ページの統計情報	32
表 4-1 : PCoIP ホストカードとゼロクライアントに対してサポートされている解像度	48
表 5-1 : オーディオパラメータ	123
表 5-2 : ネットワークパラメータ	124
表 5-3 : セッションパラメータ	124
表 5-4 : オーディオパラメータ	125
表 5-5 : ネットワークパラメータ	125
表 5-6 : セッションパラメータ	126
表 5-7 : MC ネットワーク設定パラメータ	127
表 5-8 : AWI Network ページパラメータ	130
表 5-9 : OSD Network ページパラメータ	133
表 5-10 : AWI Label ページパラメータ	135
表 5-11 : OSD Label ページパラメータ	136
表 5-12 : MC ディスカバリ設定パラメータ	138
表 5-13 : AWI Discovery ページパラメータ	139
表 5-14 : OSD Discovery ページパラメータ	141
表 5-15 : AWI SNMP ページパラメータ	142
表 5-16 : 直接セッション接続	143
表 5-17 : 直接セッション接続	143
表 5-18 : 直接セッション接続	144
表 5-19 : MC セッション設定パラメータ	145
表 5-20 : MC セッション設定パラメータ	148
表 5-21 : MC セッション設定パラメータ	150
表 5-22 : MC セッション設定パラメータ	155
表 5-23 : MC セッション設定パラメータ	159
表 5-24 : MC セッション設定パラメータ	163
表 5-25 : MC セッション設定パラメータ	167
表 5-26 : AWI Session ページパラメータ	169
表 5-27 : AWI Session ページパラメータ	171
表 5-28 : AWI Session ページパラメータ	175
表 5-29 : AWI Session ページパラメータ	179
表 5-30 : AWI Session ページパラメータ	186
表 5-31 : AWI Session ページパラメータ	192
表 5-32 : AWI Session ページパラメータ	197
表 5-33 : AWI Session ページパラメータ	202
表 5-34 : AWI Session ページパラメータ	205
表 5-35 : OSD Session ページパラメータ	209
表 5-36 : OSD Session ページパラメータ	212
表 5-37 : OSD Session ページパラメータ	215
表 5-38 : OSD Session ページパラメータ	219
表 5-39 : OSD Session ページパラメータ	223
表 5-40 : OSD Session ページパラメータ	227
表 5-41 : AWI Session ページパラメータ	231
表 5-42 : MC 暗号化設定パラメータ	233
表 5-43 : MC 帯域幅設定パラメータ	235

表 5-44 : AWI 帯域幅パラメータ	237
表 5-45 : MC 言語設定パラメータ	239
表 5-46 : AWI クライアント言語パラメータ	240
表 5-47 : OSD 言語パラメータ	241
表 5-48 : MC 言語設定パラメータ	242
表 5-49 : AWI OSD パラメータ	243
表 5-50 : OSD OSD パラメータ	244
表 5-51 : MC イメージ設定パラメータ	245
表 5-52 : AWI ホスト Image ページパラメータ	247
表 5-53 : AWI クライアント Image ページパラメータ	250
表 5-54 : OSD Image ページパラメータ	252
表 5-55 : MC モニタパラメータ	253
表 5-56 : AWI Tera1 ホストモニタパラメータ	255
表 5-57 : AWI Tera2 ホストモニタパラメータ	256
表 5-58 : MC 時間設定パラメータ	257
表 5-59 : AWI Time ページパラメータ	259
表 5-60 : MC セキュリティ設定パラメータ	260
表 5-61 : MC オーディオ承認パラメータ	262
表 5-62 : AWI Tera1 ホスト Audio ページパラメータ	263
表 5-63 : AWI クライアント Audio ページパラメータ	264
表 5-64 : MC 電源承認パラメータ	265
表 5-65 : AWI Tera1 クライアント Power ページパラメータ	266
表 5-66 : MC ホストドライバ設定パラメータ	268
表 5-67 : AWI ホストドライバ機能パラメータ	269
表 5-68 : MC イベントログ管理パラメータ	270
表 5-69 : AWI Event Log ページパラメータ	272
表 5-70 : OSD Event Log ページパラメータ	274
表 5-71 : MC 周辺機器設定パラメータ	275
表 5-72 : MC IPv6 設定パラメータ	276
表 5-73 : AWI IPv6 ページパラメータ	279
表 5-74 : OSD IPv6 ページパラメータ	280
表 5-75 : MC ディスプレイトポロジ設定パラメータ	282
表 5-76 : OSD Tera1 Display Topology ページパラメータ	286
表 5-77 : OSD Tera2 Display Topology ページパラメータ	288
表 5-78 : MC Add OSD Logo 設定パラメータ	291
表 5-79 : AWI クライアント OSD Logo Upload ページパラメータ	292
表 5-80 : MC Link to Imported Firmware パラメータ	293
表 5-81 : AWI Firmware Upload ページパラメータ	294
表 5-82 : MC プロファイルゼロクライアント USB 設定パラメータ	296
表 5-83 : Add Profile USB – Add New パラメータ	297
表 5-84 : AWI クライアント USB ページパラメータ	299
表 5-85 : USB 許可/非許可デバイスパラメータ	301
表 5-86 : USB ブリッジデバイスパラメータ	302
表 5-87 : AWI ホスト USB ページパラメータ	304
表 5-88 : USB 許可/非許可デバイスパラメータ	305
表 5-89 : MC 証明書ストア設定パラメータ	306
表 5-90 : MC Add Certificate to Store パラメータ	307
表 5-91 : AWI Certificate Upload ページパラメータ	309
表 5-92 : OSD Tera1 Display ページパラメータ	310

表 5-93 : OSD Tera2 Display ページパラメータ	313
表 5-94 : AWI Password ページパラメータ	315
表 5-95 : OSD Change Password ページパラメータ	316
表 5-96 : AWI ホスト Reset ページパラメータ	317
表 5-97 : AWI クライアント Reset ページパラメータ	317
表 5-98 : OSD Reset ページパラメータ	319
表 5-99 : AWI ホスト Session Control ページパラメータ	320
表 5-100 : AWI クライアント Session Control ページパラメータ	321
表 5-101 : AWI ホスト Session Statistics ページパラメータ	322
表 5-102 : AWI クライアント Session Statistics ページパラメータ	325
表 5-103 : OSD Session Statistics ページパラメータ	328
表 5-104 : AWI Host CPU ページパラメータ	329
表 5-105 : AWI クライアント Display ページパラメータ	330
表 5-106 : AWI PCoIP Processor ページパラメータ	331
表 5-107 : Ping ページパラメータ	333
表 5-108 : AWI Version ページパラメータ	334
表 5-109 : OSD Version ページパラメータ	335
表 5-110 : AWI ホスト : Attached Devices ページ情報	337
表 5-111 : AWI クライアント : Attached Devices ページ情報	338
表 5-112 : OSD VMware View ページパラメータ	339
表 5-113 : OSD Mouse ページパラメータ	341
表 5-114 : OSD Keyboard ページパラメータ	342
表 5-115 : OSD Touch Screen ページパラメータ	343

1 ようこそ

1.1 イントロダクション

Teradici の PCoIP ゼロクライアント/ホスト管理者ウェブヘルプへようこそ。このヘルプシステムでは、PCoIP デプロイメント内の[ホスト](#)や[ゼロクライアント](#)にアクセスして管理できるようにするための PCoIP デバイスファームウェアの設定方法について説明します。このヘルプは以下のメインセクションで構成されています。

- **最新情報**：このセクションでは、各ファームウェアリリースの新機能について説明します。各機能の詳細が記載されたトピックへのリンクが含まれています。
- **PCoIP 管理ツール**：このセクションでは、以下の PCoIP 管理ツールへのアクセス方法と使用方法について説明します。
 - **管理コンソール (MC)**：MC を使用すれば、PCoIP デプロイメント内のデバイスを集中的に制御・管理できます。このヘルプシステムでは、特定の PCoIP グループ (1 つ以上のホストまたはクライアントのセット) に割り当てるためのプロファイル (デバイス構成設定の集合) の設定方法について説明します。MC は、中規模から大規模なデプロイメントに最適なツールであり、大抵は、[コネクションブローカ](#)と組み合わせて使用されます。詳細については、「[MC について](#)」を参照してください。
 - **管理用ウェブインターフェース (AWI)**：AWI を使用すれば、インターネットブラウザから特定のクライアントまたはホストにリモートでアクセスして設定を実行することができます。詳細については、「[AWI について](#)」を参照してください。
 - **オンスクリーンディスプレイ (OSD)**：OSD はクライアントに内蔵されたグラフィカルユーザインターフェース (GUI) です。クライアントをリモートワークステーション内の仮想デスクトップまたはホストに接続するために使用されます。クライアントの設定にも使用され、MC と AWI で使用可能な設定パラメータのサブセットが用意されています。詳細については、「[OSD について](#)」を参照してください。
- **PCoIP デプロイメントシナリオ**：このセクションでは、ホストとクライアントを PCoIP ネットワークにデプロイするための最も一般的な方法を、図を使って説明します。シナリオごとの設定手順とともに、詳細を参照可能な「PCoIP GUI リファレンス」内のトピックへのリンクが含まれています。これらのシナリオは新しいデプロイメントの設定に着手する場合にとっても参考になります。
- **PCoIP GUI リファレンス**：このセクションは、MC、AWI、および OSD の各ページに表示される設定パラメータに関する詳細なリファレンスです。このリファレンスは、MC を使用してデバイスプロファイルを設定する場合や AWI または OSD を使用してデバイスを個別に設定する場合に参考にすることができます。PCoIP GUI リファレンスは MC の **Manage Profiles** ページに表示されるカテゴリ

別に編成されていますが、MC 内のページとは無関係な AWI メニューと OSD メニューに固有のセクションも含まれています。

- **PCoIP テクノロジリファレンス**：このセクションには、ヘルプシステム内で使用される一部の用語の定義が含まれています。

2 最新情報

2.1 ファームウェア 4.0.2 の最新情報

Teradici ファームウェア 4.0.2 リリースでは次のような機能の追加や強化が行われました。

- **Tera2 プロセッサファミリのサポート**：ファームウェア 4.0.2 は、表示機能、イメージング性能、メモリ、電源管理、およびその他の重要な機能が強化された新しい Tera2 プロセッサに対応しています。例えば、TERA2140 ゼロクライアントは、最大 4 台のディスプレイ（DVI-D または DisplayPort）をサポートし、リモートワークステーション用の最大 3 億ピクセル/秒（Mpps）と仮想デスクトップ用の最大 50 Mpps の速度でイメージエンコーディングを実行することができます。第 2 世代 PCoIP ゼロクライアントと、新しいプロセッサが搭載されたホストカードの詳細については、<http://www.teradici.com> にある Teradici ウェブサイトを参照してください。このファームウェアリリースでサポートされているホストカードとゼロクライアントの完全なリストについては、「[PCoIP ホストカードとゼロクライアント](#)」を参照してください。
- **プロセッサファミリ情報**：デバイス内部のプロセッサファミリやチップセットに関する情報をさまざまな方法で表示できるようになりました。詳細については、「[プロセッサ情報の表示](#)」を参照してください。
- **ディスプレイトポロジ設定の強化**：新しい Tera2 ディスプレイ機能をサポートするために、管理コンソール（MC）上の [Display Topology Configuration ページ](#) と オンスクリーンディスプレイ（OSD）上の [Display Topology](#) 設定を使用すれば、デュアルディスプレイトポロジとクアッドディスプレイトポロジのレイアウト、位置合わせ、および解像度プロパティを設定できるようになりました。
- **優先解像度オーバーライドの強化**：このリリースでは、デフォルトの拡張ディスプレイ識別データ（EDID）情報をホストワークステーション内のグラフィックスプロセッシングユニット（GPU）にアダプタイズするようにゼロクライアントを設定するときの、デフォルト解像度の拡張リストが追加されています。Tera2 クライアントでは、最大 4 台のディスプレイの優先（デフォルト）解像度を設定することができます。詳細については、「[OSD Tera2：ディスプレイ設定](#)」を参照してください。
- **テストディスプレイ解像度の拡張リスト**：管理用ウェブインターフェース（AWI）の **Display** ページに、ゼロクライアント上でテストパターンを確認する場合のディスプレイ解像度の拡張リストが表示されるようになりました。テストパターンの設定方法については、「[AWI クライアント：ディスプレイ設定](#)」を

参照してください。

- **新しい Tera2 切断オプション**：ユーザがリモートワークステーションとのセッション中に、Tera2 ゼロクライアント上の接続/切断ボタンを押すと、新しいダイアログがポップアップ表示され、セッションを切断するか、リモートワークステーションの電源をオフにするかを選択することができます。このポップアップダイアログは、Ctrl+Alt+F12 ホットキーシーケンスを使用して表示することもできます。この新機能の詳細については、「[セッションの切断](#)」を参照してください。
- **OSD メッセージングの拡張**：OSD 上のメッセージングが拡張され、新しいオーバーレイウィンドウと新しいインラインメッセージが OSD の **Connect** ページに表示されるようになりました。例えば、ユーザがユーザ名またはパスワードを間違えて入力した場合や Caps Lock キーがオンになっている場合は、このページの **Connect** ボタンの上にユーザに対する警告メッセージが表示されます。ネットワーク接続の消失/ダウン/アップメッセージもこの場所に表示され、右下のネットワークアイコンの表示が変化します。詳細については、「[セッションへの接続](#)」と「[オーバーレイウィンドウ](#)」を参照してください。
- **管理コンソールのキャッシュ対象 VCS アドレスの拡張**：管理コンソールの **Session Configuration – View Connection Server** ページで、キャッシュ対象 View Connection Server アドレスを 25 個まで設定できるようになりました。これらのサーバは、ユーザが VMware View Connection Server を使用して仮想デスクトップに接続しているときに OSD **Connect** ページのドロップダウンリストに表示されます。詳細については、「[MC : View Connection Server セッション設定](#)」を参照してください。
- **Imprivata OneSign 設定の強化**：**View Connection Server – Imprivata OneSign** ページの新しいパラメータを使用すれば、OneSign サーバのデスクトップ名を設定することができます。デスクトッププールリストにこの名前を持つプールが含まれているときに、ゼロクライアントがこのデスクトップとのセッションを開始します。[MC : View Connection Server + Imprivata OneSign](#) ページでこのオプションを使用してプロファイルを設定することも、[AWI Client : view Connection Server + Imprivata Onesign](#) ページまたは [OSD : View Connection Server + Imprivata Onesign](#) ページで特定のゼロクライアントを設定することもできます。
- **管理者用オンラインヘルプ**：このリリースでは、PCoIP ゼロクライアント/ホストカード管理者マニュアルがオンラインヘルプとして配布されており、この中に PCoIP 管理者ツール (MC、AWI、および OSD) を使用したデバイスファームウェアの設定方法を含む完全な GUI リファレンスが掲載されています。また、一般的な PCoIP デバイスデプロイメントシナリオに関するトピックも掲載されており、図、説明、およびそれぞれの設定詳細へのリンクが提供されます。

3 PCoIP 管理ツール

3.1 MC について

PCoIP 管理コンソール (MC) を使用すれば、PCoIP デプロイメント内のデバイスを集中的に管理することができます。このコンソールは VMware Player 上で動作する VMware® 仮想マシン (VM) としてパッケージ化されています。この MC は、デバイスのステータス情報を確認したり、グループやプロファイルを作成したり、グループ (同じ設定が必要な 1 つ以上のデバイス) に適用可能なプロファイル (構成設定の集合) を設定したり、証明書やファームウェアをデバイスにアップロードしたり、デバイスの電源設定を制御したり、デバイスイベントログの監視を管理したりするために使用することができます。

このヘルプシステム内の MC トピックでは、MC を使用したデバイスプロファイルの設定方法について説明します。MC のインストール、セットアップ、および使用方法については、『PCoIP Management Console User Manual』 (TER0812002) を参照してください。

MC ウェブインターフェースの IP アドレスを Internet Explorer または Mozilla Firefox ブラウザに入力すると、ブラウザから HTTPS (SSL ソケット経由の HTTP) を使用して MC ウェブインターフェースに接続されます。MC ウェブインターフェースの IP アドレスはインストール後の MC 仮想マシンコンソールから (静的にまたは DHCP 経由で) 設定します。MC へのアクセスは管理パスワードを使用して制御されます。このパスワードもインストール後の MC 仮想マシンコンソールから設定します。これらのセットアップ手順の詳細は、『PCoIP Management Console User Manual』 (TER0812002) に記載されています。

MC の HTTPS 接続は、PCoIP MC ルート認証局 (CA) 証明書を使用して保護されます。この証明書のインストール方法については、『PCoIP Management Console User Manual』 (TER0812002) を参照してください。

このリリースを使用してテスト済みのブラウザは次のとおりです。

- Firefox バージョン 3 以降
- Internet Explorer 7.0 および 8.0

上記以外のブラウザを使用して MC ウェブインターフェースにログインしようとすると、エラーメッセージとともにサポートされているブラウザのリストが表示されます。

3.2 MC へのログイン

管理コンソールウェブインターフェースにログインするには：

1. インターネットブラウザに MC ウェブページの IP アドレスを入力します。この IP アドレスは、MC の設定方法に応じて、静的アドレスにも動的アドレスにもすることができます。
 - **静的 IP アドレス**：IP アドレスがハードコードされるため、覚えておく必要があります。
 - **動的 IP アドレス**：IP アドレスが動的ホスト構成プロトコル（DHCP）サーバによって動的に割り当てられます。IP アドレスは DHCP サーバから入手することができます。
2. ログインページで、管理パスワードを入力します。デフォルト値は空白（つまり、""）です。



図 3-1 : MC ログインページ

3. MC に初めてログインした場合は、使用許諾契約書の受け入れを要求するプロンプトが表示されます。契約書の内容を読んでから、このページの **Agree** をクリックします。これ以降のログインではこのプロンプトが表示されません。

MC にログインすると、[Home](#) ページが表示されます。

3.3 MC Home ページ

MC Home ページには、全 MC 機能へのリンクの他に、MC で検出された PCoIP デバイスに関する概要情報を含む **Site Status** セクションも表示されます。

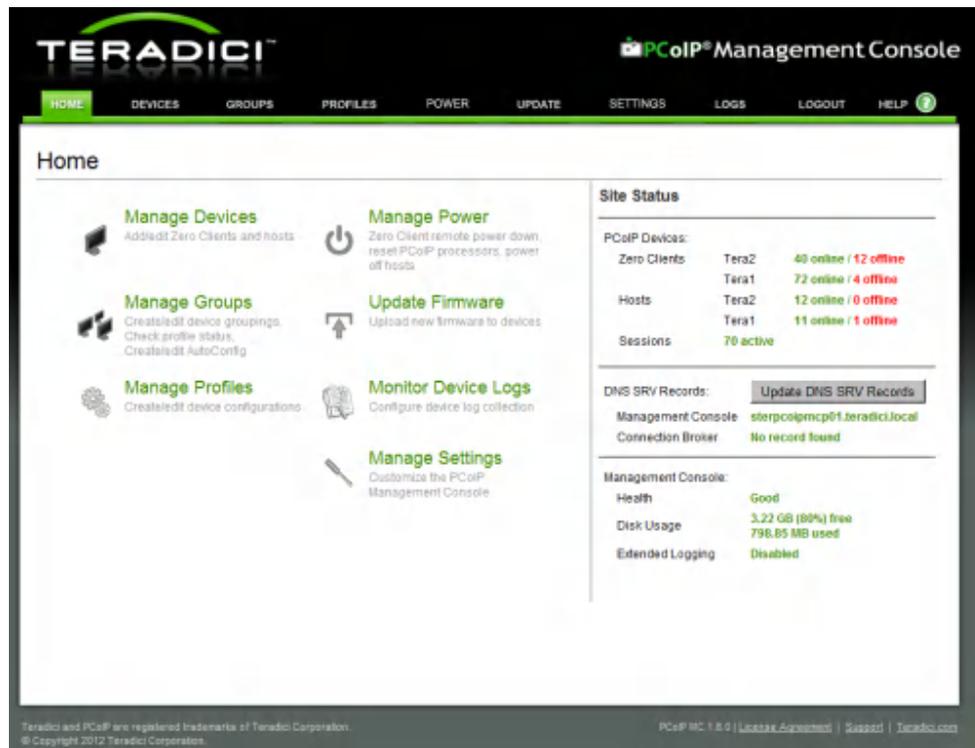


図 3-2 : MC Home ページ

デバイスファームウェアは、MC 上でプロファイルを定義してからそれをデバイスのグループに適用することによって設定されます。**Profiles** タブをクリックすると、システム内のプロファイルを管理するための **Profile Management** ページが表示されます。

3.4 MC Profile Management ページ

Profile Management ページでは、プロファイルを表示、追加、複製、設定（つまり、そのプロパティの設定）、編集、削除、およびエクスポートすることができます。

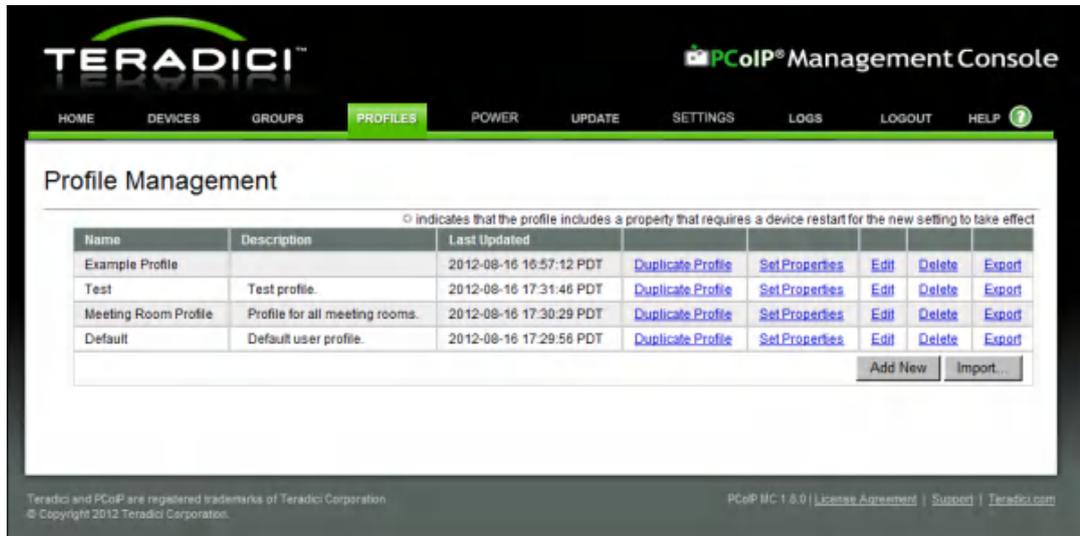


図 3-3 : MC Profile Management ページ

プロファイルを作成したら、**Set Properties** リンクをクリックして [Manage Profiles](#) ページを表示し、プロファイルのデバイス設定の定義を開始することができます。

3.5 MC Manage Profiles ページ

下の図は、特定のプロファイルの **Manage Profiles** ページを示しています。このページには、デバイスファームウェアの設定に使用されるすべてのカテゴリのリストが表示されます。

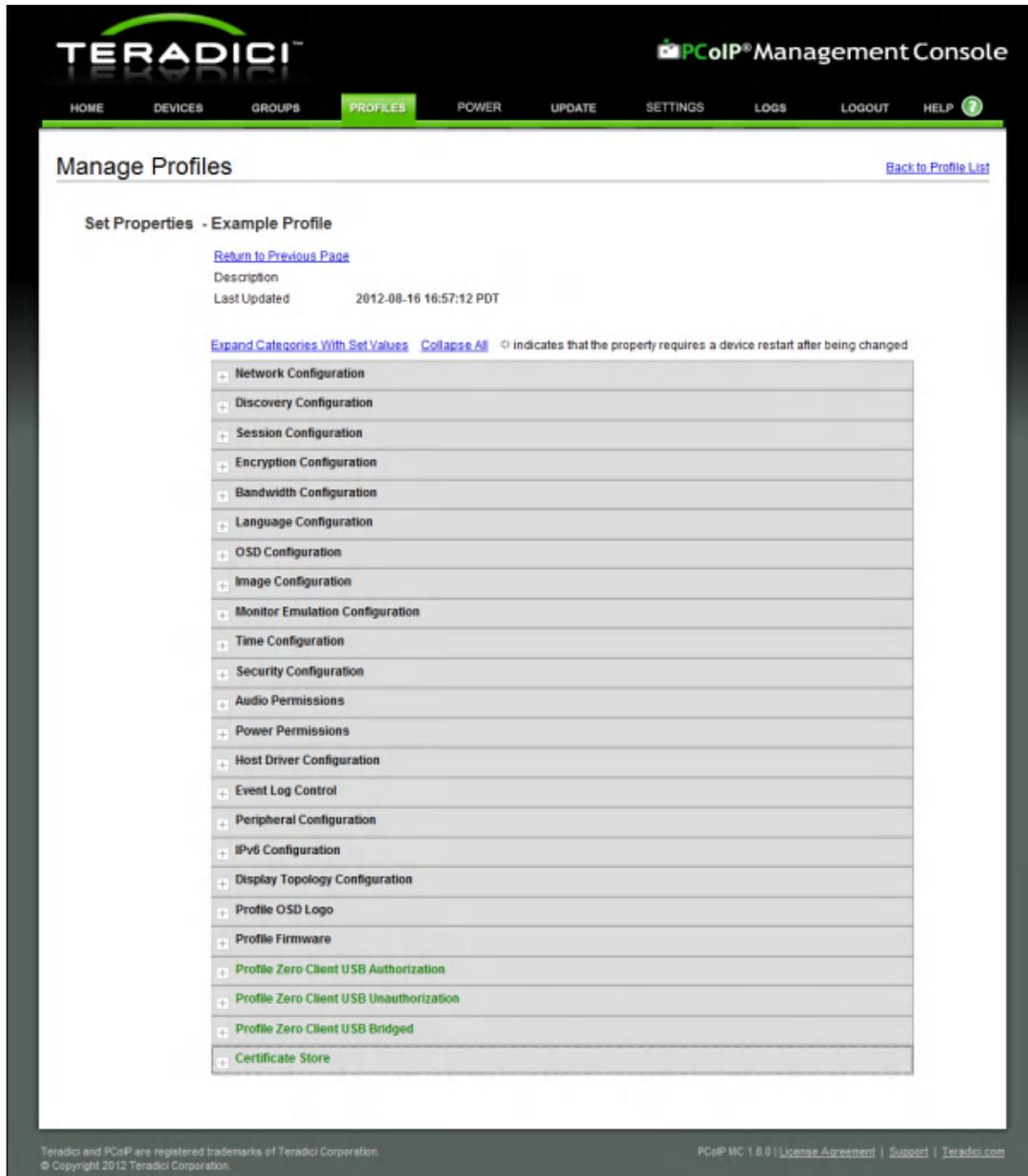


図 3-4 : MC Manage Profiles ページ

カテゴリを設定するには、下の例で示すように、それを展開して、**Edit Properties** リンクをクリックします。

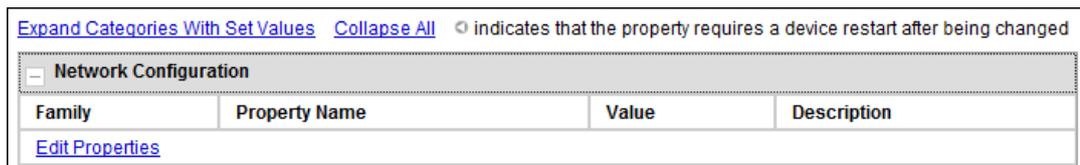
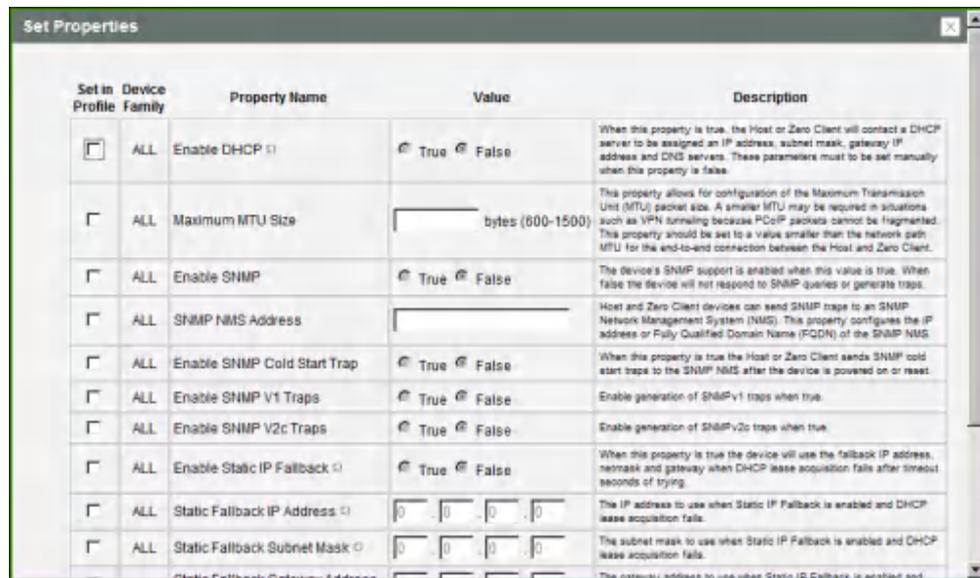


図 3-5 : Edit Properties リンク

このリンクは、そのカテゴリの **Set Properties** ページを表示します。このページでカテゴリの個々のパラメータを設定することができます。下の例は、**Network Configuration** カテゴリのパラメータを示しています。



Set in Profile	Device Family	Property Name	Value	Description
<input type="checkbox"/>	ALL	Enable DHCP	<input checked="" type="radio"/> True <input type="radio"/> False	When this property is true, the Host or Zero Client will contact a DHCP server to be assigned an IP address, subnet mask, gateway IP address and DNS servers. These parameters must be set manually when this property is false.
<input type="checkbox"/>	ALL	Maximum MTU Size	<input type="text"/> bytes (800-1500)	This property allows for configuration of the Maximum Transmission Unit (MTU) packet size. A smaller MTU may be required in situations such as VPN tunneling because PCoIP packets cannot be fragmented. This property should be set to a value smaller than the network path MTU for the end-to-end connection between the Host and Zero Client.
<input type="checkbox"/>	ALL	Enable SNMP	<input checked="" type="radio"/> True <input type="radio"/> False	The device's SNMP support is enabled when this value is true. When false the device will not respond to SNMP queries or generate traps.
<input type="checkbox"/>	ALL	SNMP NMS Address	<input type="text"/>	Host and Zero Client devices can send SNMP traps to an SNMP Network Management System (NMS). This property configures the IP address or Fully Qualified Domain Name (FQDN) of the SNMP NMS.
<input type="checkbox"/>	ALL	Enable SNMP Cold Start Trap	<input checked="" type="radio"/> True <input type="radio"/> False	When this property is true the Host or Zero Client sends SNMP cold start traps to the SNMP NMS after the device is powered on or reset.
<input type="checkbox"/>	ALL	Enable SNMP V1 Traps	<input checked="" type="radio"/> True <input type="radio"/> False	Enable generation of SNMPv1 traps when true.
<input type="checkbox"/>	ALL	Enable SNMP V2c Traps	<input checked="" type="radio"/> True <input type="radio"/> False	Enable generation of SNMPv2c traps when true.
<input type="checkbox"/>	ALL	Enable Static IP Fallback	<input checked="" type="radio"/> True <input type="radio"/> False	When this property is true the device will use the fallback IP address, netmask and gateway when DHCP lease acquisition fails after timeout seconds of trying.
<input type="checkbox"/>	ALL	Static Fallback IP Address	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	The IP address to use when Static IP Fallback is enabled and DHCP lease acquisition fails.
<input type="checkbox"/>	ALL	Static Fallback Subnet Mask	<input type="text"/> . <input type="text"/> . <input type="text"/> . <input type="text"/>	The subnet mask to use when Static IP Fallback is enabled and DHCP lease acquisition fails.

図 3-6 : ネットワーク設定用の **Set Properties** ページ

注意：カテゴリごとのパラメータテーブルには各パラメータの説明が記載された **Description** 列があります。これらのパラメータについては GUI リファレンスの **MC** セクションにも説明があります。

必要なプロパティの設定が完了すると、**Manage Profiles** ページでカテゴリが拡張され、それらの設定が表示されます。展開/折りたたみリンクを使用してこの情報の表示を制御することができます。

いくつかのカテゴリが設定されたプロファイルの例を以下に示します。

Manage Profiles [Back to Profile List](#)

Set Properties - Example Profile

[Return to Previous Page](#)
 Description
 Last Updated 2012-08-22 10:47:40 PDT

[Expand Categories With Set Values](#) [Collapse All](#) indicates that the property requires a device restart after being changed

Network Configuration

Family	Property Name	Value	Description
ALL	Enable DHCP <input type="checkbox"/>	False	When this property is true, the Host or Zero Client will contact a DHCP server to be assigned an IP address, subnet mask, gateway IP address and DNS servers. These parameters must be set manually when this property is false.

[Edit Properties](#)

Discovery Configuration

Session Configuration

Encryption Configuration

Bandwidth Configuration

Language Configuration

Family	Property Name	Value	Description
ALL	Language <input type="checkbox"/>	English	This property configures the language of the OSD. The drop down menu lists the supported languages.

[Edit Properties](#)

OSD Configuration

Family	Property Name	Value	Description
--------	---------------	-------	-------------

[Edit Properties](#)

Image Configuration

Monitor Emulation Configuration

Time Configuration

Family	Property Name	Value	Description
ALL	NTP Server Hostname	10.64.224.50	This property identifies the Network Time Protocol (NTP) server the Host or Zero Client will contact to determine the current time. This property can be entered as either an IP address or a Fully Qualified Domain Name.
ALL	Enable DST	True	When this property is true the Host or Zero Client adjusts the current time based on daylight savings.
ALL	Time Zone Offset	gmt_minus_0800_pacific_time	This property configures the time zone.

[Edit Properties](#)

Security Configuration

Audio Permissions

Power Permissions

Host Driver Configuration

Event Log Control

Family	Property Name	Value	Description
ALL	Syslog Server Hostname	10.64.16.104	This property identifies the Syslog server the Host or Zero Client will send event log messages to. This property can be entered as either an IP address or a Fully Qualified Domain Name.

[Edit Properties](#)

Peripheral Configuration

IPv6 Configuration

Display Technology Configuration

図 3-7 : MC Manage Profiles ページ – 設定後

このヘルプシステムの GUI リファレンスに各カテゴリの詳細が記載されています。これらの MC ページを使用してデバイスを設定または管理する方法については、GUI リファレンスの該当するセクションを参照してください。

プロファイルの適用方法については、『PCoIP Management Console User Manual』(TER0812002)を参照してください。

3.6 AWI について

PCoIP 管理用ウェブインターフェース (AWI) を使用すれば、PCoIP ホストまたはクライアントとリモートでデータをやり取りすることができます。AWI では、ホストまたはクライアントを管理および設定したり、それらに関する重要な情報を表示したり、それらにファームウェアや証明書をアップロードしたりすることもできます。

デバイスの IP アドレスを Internet Explorer または Mozilla Firefox ブラウザに入力すると、ブラウザから HTTPS (SSL ソケット経由の HTTP) を使用してデバイスの AWI ウェブページに接続されます。AWI へのアクセスは、管理パスワードを使用して制御されます。このパスワードはいつでも無効にすることができます。

AWI の HTTPS 接続は、PCoIP MC ルート認証局 (CA) 証明書を使用して保護されます。AWI にログインしたときの警告メッセージを避けるために、この証明書はブラウザでインストールすることをお勧めします。証明書ファイル ("cacert.pem") はファームウェアリリースに含まれていますが、[Teradici サポートサイト](#)から直接ダウンロードすることもできます。証明書のインストール手順については、Teradici サポートサイトで知識ベースサポートトピック 15134-529 を参照してください。

このリリースを使用してテスト済みのブラウザは次のとおりです。

- Firefox バージョン 3 以降
- Internet Explorer 7.0 および 8.0

3.7 AWI へのログイン

ホストまたはクライアントの管理用ウェブインターフェースウェブページにログインするには：

1. インターネットブラウザで、ホストまたはクライアントの IP アドレスを入力します。IP アドレスは、IP ネットワーク内の IP アドレスの決定方法に応じて、静的アドレスにも動的アドレスにもすることができます。
 - **静的 IP アドレス**：IP アドレスがハードコードされるため、覚えておく必要があります。
 - **動的 IP アドレス**：IP アドレスが動的ホスト構成プロトコル (DHCP) サーバによって動的に割り当てられます。IP アドレスは DHCP サーバから入手することができます。
2. **Log In** ページで、管理パスワードを入力します。デフォルト値は空白 (つまり、" ") です。

Log In

Please enter the administrative password to access this device.

Password:

Idle Timeout:

図 3-8 : AWI Log In ページ

3. アイドルタイムアウト（デバイスが自動的にログオフされるまでの時間）を変更するには、**Idle Timeout** ドロップダウンメニューからオプションを選択します。
4. **Log In** をクリックします。

注意：DHCP 使用しているネットワークによっては、[PCoIP デバイス名](#)を使用して AWI にアクセスできる場合があります。

注意：パスワード保護が無効になっている PCoIP デバイスの場合は、ログイン時にパスワードが要求されません。パスワード保護は MC の **Manage Profiles** ページの [セキュリティ設定](#) を通して有効または無効にすることができます。

ファームウェアデフォルトに設定されている場合は、初めてのログイン時に **Initial Setup** ページが表示されます。このページではオーディオ、ネットワーク、およびセッションの各パラメータを設定することができます。**Apply** をクリックすると、以降のセッションごとに **Home ページ** が表示されます。このページではデバイスステータスの概要が提供されます。

ログインしようとして警告メッセージが表示された場合は、そのデバイス上で既にセッションが進行中です。一度にデバイスにログインできるのは 1 人のユーザだけです。新しいセッションがログインすると、現在のセッションが終了して、1 つ前のユーザが **Log In** ページに戻ります。

3.8 AWI Initial Setup ページ

AWI の **Initial Setup** ページには、クライアントまたはホストデバイスを使用する前に設定しなければならないオーディオ、ネットワーク、およびセッションの設定パラメータが表示されます。このページは、初期セットアップを簡略化して、新しいユーザが PCoIP ゼロクライアントとリモートワークステーション内の PCoIP ホストカード間でセッションを確立する時間の短縮を支援します。

AWI の [クライアント Initial Setup](#) ページと [ホスト Initial Setup](#) ページは同じではありません。それぞれのページにクライアントとホストに適用されるパラメータが表示されます。

ファームウェアデフォルトに設定されている場合は、初めてのログイン時に **Initial Setup** ページが表示されます。**Apply** をクリックすると、ファームウェアパラメータがリセットされていなければ、以降のセッションで [Home](#) ページが表示されます。

注意：ホストディスクバリまたは接続管理システムを使用しているより複雑な環境では、**Initial Setup** ページで使用可能なその他の設定が必要になります。

3.9 AWI Home ページ

AWI Home ページには、ホストまたはクライアントに関する統計情報の概要が表示されます。メニューバーの左上のセクションにある **Home** リンクをクリックすれば、いつでも **Home** ページを表示することができます。



The screenshot shows the PCoIP Host Card page with the following content:

Log Out **PCoIP® Host Card**

Home Configuration / Permissions / Diagnostics / Info / Upload

PCoIP®

PCoIP® Host Card

PCoIP® device status and statistics for the current session.

Processor: TERA2240 revision 1.0 (512 MB)
Time Since Boot: 0 Days 3 Hours 4 Minutes 0 Seconds
PCoIP Device Name: pcoip-host-0030040deb9b

Connection State: Connected to TERA2140 client [192.168.54.133](#)
802.1X Authentication Status: Disabled
Session Encryption Type: AES-256

PCoIP Packets (Sent/Received/Lost): 15696 / 10944 / 0
Bytes (Sent/Received): 6299360 / 1452576
Round Trip Latency (Min/Avg/Max): 2 / 4 / 5 ms
Transmit Bandwidth (Min/Avg/Max/Limit): 8 / 280 / 4232 / 8464 kbps
Receive Bandwidth (Min/Avg/Max): 0 / 56 / 392 kbps

Pipeline Processing Rate (Avg/Max/Limit): 3 / 39 / 297 Mpps
Endpoint Image Settings In Use: Client
Initial Image Quality (Min/Active/Max): 40 / 90 / 90
Image Quality Preference: 50
Build To Lossless: Enabled

Display	Maximum Rate: Refresh Rate	Input Change Rate	Output Process Rate	Image Quality
1	60 fps	7 fps	7 fps	Perceptually Lossless
2	N/A	N/A	N/A	N/A
3	60 fps	0 fps	0 fps	Lossless
4	N/A	N/A	N/A	N/A

図 3-9 : AWI ホスト : Home ページ



図 3-10 : AWI クライアント : Home ページ

注意：上の図は、4 台のディスプレイを接続可能なデバイスに関するセッション統計情報を示しています。デプロイメントで 2 台のディスプレイしかサポートされていない場合は、その 2 台のディスプレイに関する情報がページの下部領域に表示されます。

表 3-1 : AWI Home ページの統計情報

統計情報	説明
Processor	PCoIP プロセッサのタイプ、バージョン、および RAM サイズ
Time Since Boot	PCoIP プロセッサが動作していた時間長

統計情報	説明
PCoIP Device Name	デバイスの論理名。 このフィールドは、DHCP が有効になっている場合またはシステムが DNS サーバへのホスト名登録をサポートするように設定されている場合に、ホストまたはクライアントが DNS サーバに登録する名前です（ Label ページの PCoIP Device Name パラメータを参照してください）。
Connection State	PCoIP セッションの現在（または最後）の状態。値には以下が含まれます。 <ul style="list-style-type: none"> • Asleep • Canceling • Connected • Connection Pending • Disconnected • Waking
802.1X Authentication Status	デバイス上で 802.1X 認証が有効になっているか、無効になっているかを示します。
Session Encryption Type	セッションがアクティブ時に使用される暗号化のタイプ： <ul style="list-style-type: none"> • AES-128-GCM • SALS20-256-Round 12
PCoIP Packets Statistics	<p>PCoIP Packets Sent : 現在/最後のセッションで送信された PCoIP パケットの総数。</p> <p>PCoIP Packets Received : 現在/最後のセッションで受信された PCoIP パケットの総数。</p> <p>PCoIP Packets Lost : 現在/最後のセッションで消失された PCoIP パケットの総数。</p>
Bytes	<p>Bytes Sent : 現在/最後のセッションで送信されたバイトの総数。</p> <p>Bytes Received : 現在/最後のセッションで受信されたバイトの総数。</p>
Round Trip Latency	PCoIP システムとネットワークの往復遅延の最小値、平均値、および最大値（ミリ秒 (+/- 1 ms) 単位）
Bandwidth Statistics	<p>Transmit Bandwidth : Tera プロセッサによって送信された最小、平均、および最大トラフィック。有効帯域幅限界は Tera プロセッサが生成する可能性のあるネットワークトラフィックの最大量です。この値は、設定された帯域幅パラメータと現在（または最後）のネットワークの混雑レベルから抽出されます。</p> <p>Receive Bandwidth : Tera プロセッサによって受信された最小、平均、および最大トラフィック。</p>

統計情報	説明
Pipeline Processing Rate	イメージエンジンによって現在処理されているイメージデータの容量（メガピクセル数/秒単位）。
Endpoint Image Settings In Use	使用されているイメージ設定がクライアントで設定されたのか、ホストで設定されたのかを示します。これは、ホストデバイスの Image ページで Use Client Image Settings フィールドがどのように設定されているかに基づきます。
Image Quality	最低品質設定と最高品質設定はデバイスの Image ページから取得されます。 アクティブ設定は現在セッションで使用されている設定で、ホスト上にのみ表示されます。
Image Quality Preference	この設定は、 Image ページの Image Quality Preference フィールドから取得されます。この値は、イメージがよりスムーズなイメージに設定されているのか、よりシャープなイメージに設定されているのかを示します。
Build to Lossless	このフィールドに表示されるオプションには以下が含まれます。 Enabled : Image ページの Disable Build to Lossless フィールドがオフになっています。 Disabled : Disable Build to Lossless フィールドがオンになっています。
Display	ディスプレイのポート番号。
Maximum Rate	この列は取り付けられたディスプレイのリフレッシュレートを表します。 Image ページの Maximum Rate フィールドが 0（つまり、無制限）に設定されている場合は、最大レートがモニタのリフレッシュレートから取得されます。 Image ページの Maximum Rate フィールドが 0 より大きい値に設定されている場合は、リフレッシュレートが "User Defined" として表示されます。
Input Change Rate	GPU からのコンテンツ変更率。これには、ユーザが実行しているすべてのもの（カーソル移動、電子メール編集、ストリーミングビデオなど）が含まれます。 注意：このオプションはホスト上でのみ使用することができます。クライアント上には表示されません。
Output Process Rate	ホスト上のイメージエンジンからクライアントに現在送信されているフレームレート。

統計情報	説明
Image Quality	取り付けられたディスプレイの現在のロスレス状態を示します。 <ul style="list-style-type: none"> • Lossy • Perceptually lossless • Lossless

注意：ホストの [Session Statistics](#) ページまたはクライアントの [Session Statistics](#) ページで **Reset Statistics** ボタンをクリックすると、**Home** ページに報告される統計情報もリセットされます。

3.10 AWI メニュー

AWIには、さまざまな設定ページとステータスページにリンクされた5つのメインメニューがあります。

- **Configuration** : このメニュー下のページを使用すれば、ネットワーク設定、言語、セッションパラメータなど、デバイスのさまざまな側面を設定することができます。
- **Permissions** : このメニュー下のページを使用すれば、クライアント上のUSB、オーディオ、および電源に対する承認とホスト上のUSBとオーディオに対する承認をセットアップすることができます。
- **Diagnostics** : このメニュー下のページを使用すれば、デバイスのトラブルシューティングが支援されます。
- **Info** : このメニュー下のページを使用すれば、ファームウェア情報と現在デバイスに接続されているデバイスを表示することができます。
- **Upload** : このメニュー下のページを使用すれば、新しいファームウェアバージョン、OSD ロゴ、および証明書をデバイスにアップロードすることができます。

下の図は、AWIで使用可能なメニューとページを示しています。

注意：クライアントからしか使用できないページには (*C) が付けられ、ホストからしか使用できないページには (*H) が付けられています。

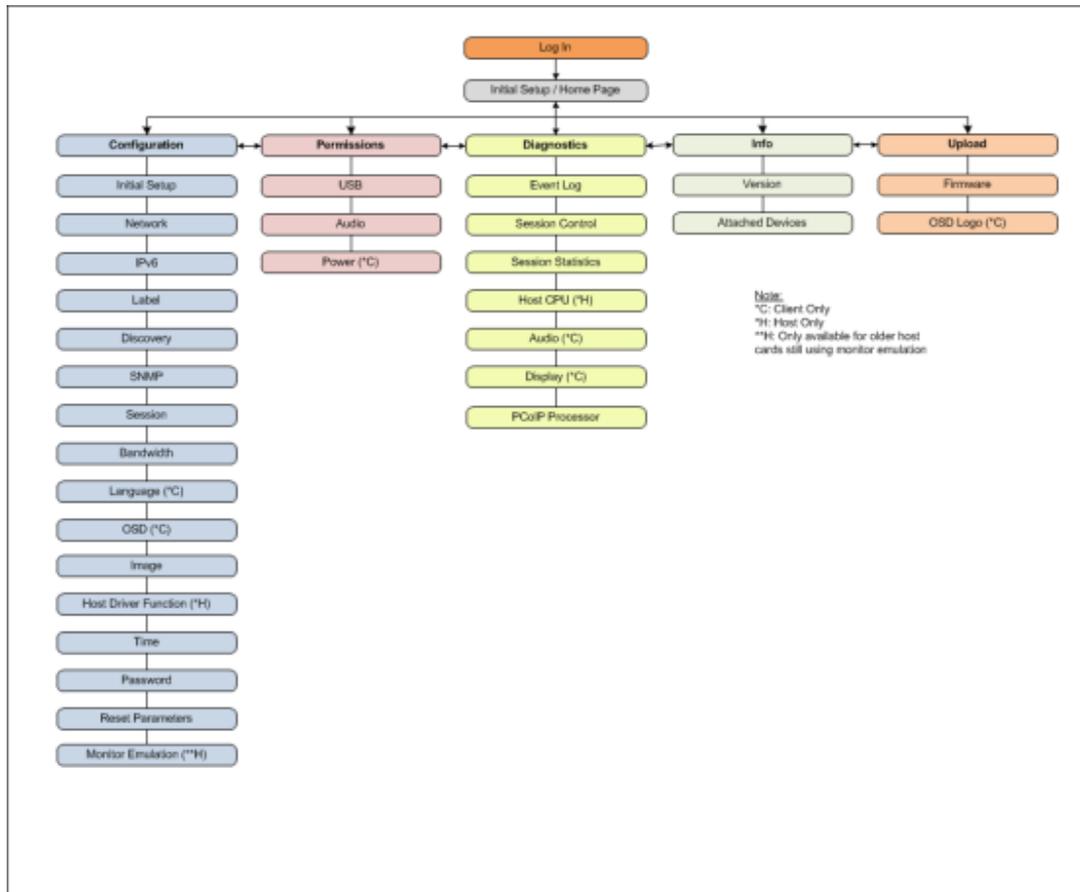


図 3-11 : AWI メニューの概要

このヘルプシステムの GUI リファレンスに各ページの詳細が記載されています。これらの AWI ページを使用してデバイスを設定または管理する方法については、GUI リファレンスの該当するセクションを参照してください。

3.11 OSD について

下の図に示す PCoIP オンスクリーンディスプレイ (OSD) は、クライアントに内蔵されたグラフィカルユーザインターフェース (GUI) です。この画面はクライアントの電源がオンになっており、PCoIP セッションが始まっていない場合に表示されます。この唯一の例外は、クライアントが管理起動または自動再接続に設定されている場合です。



図 3-12 : OSD メインウィンドウ

左上の **Options** メニューを使用すれば、クライアントを設定したり、それに関する情報を表示したりするためのさまざまなサブメニューにアクセスすることができます。ウィンドウの中央にある **Connect** ボタンを使用すれば、クライアントを仮想デスクトップまたはリモートワークステーション内のホストカードに接続することができます。

3.12 セッションへの接続

OSD を使用すれば、**Connect** ウィンドウの中央にある緑色の **Connect** ボタンをクリックすることにより、クライアントとリモートワークステーション内のホストカード間（またはクライアントと仮想デスクトップ間）でセッションを構築することができます。接続が確立されると、OSD のローカル GUI が消去され、セッションイメージが表示されます。

下の図は、**Direct to Host** セッションタイプ、つまり、クライアントがリモートワークステーション内のホストカードに接続している場合の **Connect** ウィンドウを示しています。



図 3-13 : OSD Direct to Host 接続ウィンドウ

ネットワーク接続が初期化中に、次のような進捗を示すさまざまなステータスメッセージがボタンの上に表示されます。



図 3-14 : OSD 接続ステータス

起動中に問題が発生した場合、例えば、接続が確立されなかったり、DHCP リースに失敗したりした場合は、問題の特徴を示す別のメッセージがこの領域に表示されます。

下の図は、View Connection Server 接続用、つまり、クライアントが VMware View Connection Server を使用して仮想デスクトップに接続している場合の **Connect** ウィンドウを示しています。



図 3-15 : OSD View Connection Server 接続ウィンドウ

注意 : **Connect** ボタンの上に表示されるロゴは、クライアントの AWI から [Upload > OSD Logo](#) メニューを使用して交換イメージをアップロードすることにより、変更することができます。

接続の初期化中は、ユーザに接続の進捗を報告するため、または、ユーザに問題を警告するためのステータスメッセージが **Connect** ボタンの上に表示される場合があります。

View Connection Server に接続すると、次のような仮想デスクトップのログインページが表示されます。



図 3-16 : 仮想デスクトップのログインページ

ユーザ名とパスワードが間違っていて入力された場合、または、**Caps Lock** キーがオンになっている場合は、これらの問題を示すメッセージがこのページに表示されます。

VMware View Connection Server 用の正しい信頼できる SSL ルート証明書がクライアントにインストールされていない場合は、次のような警告が表示されます。



図 3-17 : OSD View Connection Server 証明書の警告

この警告でユーザが **Continue** をクリックすると、セッションが保護されません。このことは、ウィンドウの左上にある錠前上の警告アイコンと同時に、赤色の取り消し線付きの "https" によって示され、セキュアな HTTPS プロトコルが接続に使用されないことがユーザに伝達されます。



図 3-18 : 安全でない警告が表示された OSD ログイン画面

管理者であれば、次に示す [Options > User Settings > VMware View](#) ページを使用して、検証不可能なサーバへの接続を拒否するようにゼロクライアントを設定することにより、ユーザが安全でないセッションを開始できないようにすることができます。

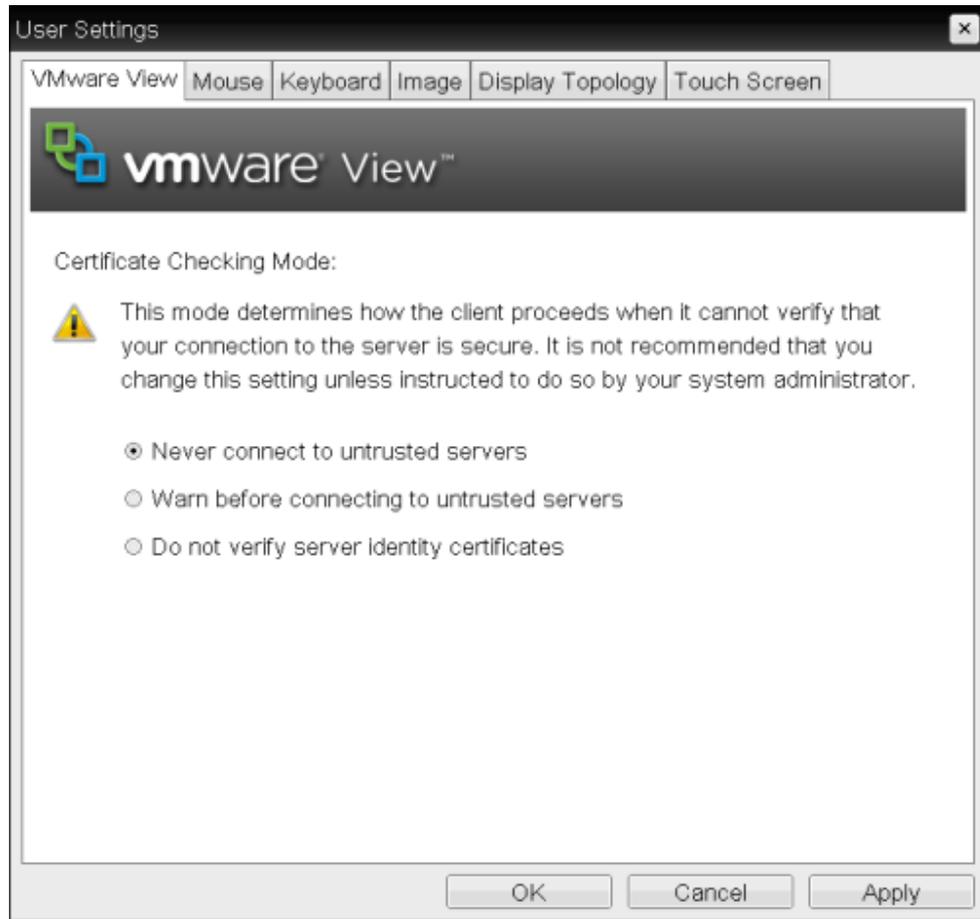


図 3-19 : OSD VMware View ページ

AWI を使用すれば、**Session – View Connection Server** ページで [VCS Certificate Check Mode Lockout](#) を有効にして、ユーザがこの設定を変更できないようにすることができます。

関連項目：

- MC を使用して証明書をプロファイルにアップロードする方法については、「[MC：証明ストア管理](#)」を参照してください。
- AWI を使用して証明書をデバイスに個別にアップロードする方法については、「[AWI：証明書アップロード設定](#)」を参照してください。
- 起動中またはセッション確立後のユーザセッションの上部に表示されるその他の OSD メッセージの詳細については、「[オーバーレイウィンドウ](#)」を参照してください。

3.13 セッションの切断

Tera1 クライアントの場合は、デバイス上の接続/切断ボタンを押すことによって、セッションを切断して OSD に戻ることができます。

Tera2 クライアントの場合は、デバイスの接続/切断ボタンを押すことによって、仮想デスクトップセッションを切断して OSD に戻ることができます。ただし、リモートワークステーション内のホストカードとのセッション中にこのボタンを押すと、下の図に示すように、Zero Client Control Panel オーバーレイが開いて、セッションを切断する、リモートワークステーションの電源をオフにする、または操作をキャンセルするためのオプションが表示されます。



図 3-20 : Zero Client Control Panel

ユーザは次のような方法でこのオーバーレイからオプションを選択できます。

- 接続/切断ボタンをタップしながらオプションを切り替えて必要なオプションが強調表示されたら、確定するまで4秒のカウントダウンを待ちます。
- キーボードの上/下矢印キーを使用して必要なオプションを強調表示してから、Enter キーを押します。
- 必要なオプションの番号を入力して直接選択します。

以下のオプションが事前に設定されていれば、セッション中に、Ctrl+Alt+F12 ホットキーシーケンスを使用してこのオーバーレイを表示することもできます。

- **Session – View Connection Server** ページの詳細オプション内の [Enable Session Disconnect Hotkey](#) を有効にする必要があります。
- ホストコンピュータ上の PCoIP ホストソフトウェアで **Enable Local Cursor and Keyboard** 機能を有効にする必要があります。詳細については、『PCoIP Host Software User Guide』（TER0810001）を参照してください。
- クライアント上で、キーボードがローカルに接続されている（つまり、ブリッジされていない）ことが認識されている必要があります。

注意：後の2つのオプションは、上/下矢印キーを使用するか、番号を入力することによってこのオーバーレイ上の切断オプションを選択できるように設定しておく必要もあります。

2番目のオーバーレイオプション（ワークステーションの電源をオフにする）を使用できるようにするには、「ハード」電源オフを許可するようにクライアント上の

電源承認を設定する必要があります。このパラメータは MC [Power Permissions](#) ページまたは AWI [Power Permissions](#) ページから設定することができます。

3.14 オーバーレイウィンドウ

オーバーレイウィンドウは、状態が変化したとき、例えば、ネットワーク接続が失われたり、未承認の USB デバイスがプラグインされたりした場合に、関連情報を伝達するためにユーザの PCoIP セッションに対して表示される場合があります。このオーバーレイには、下の例に示すように、ネットワーク、USB デバイス、およびモニタのステータスがアイコンとテキストで表示されます。

3.14.1 Display Link Training Failed

このオーバーレイは、DisplayPort ディスプレイインターフェース (DVI インターフェースの対するもの) を備えた Tera2 クライアント上にのみ表示されます。DisplayPort プロトコルでは、さまざまなケーブル長や信号品質に適合するためのリンクトレーニングシーケンスが必要です。このトレーニングに失敗した場合は、「Display link training failed」というメッセージを含む以下のオーバーレイが表示されます。

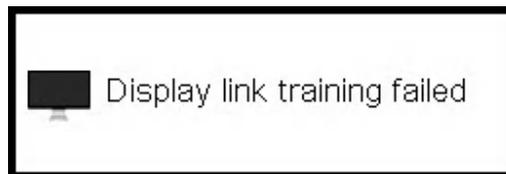


図 3-21 : Display Link Training Failed オーバーレイ

3.14.2 Half Duplex オーバーレイ

PCoIP テクノロジは半二重ネットワーク接続と互換性がありません。半二重接続が検出された場合は、「Half-duplex network connection」というメッセージを含む以下のオーバーレイが表示されます。

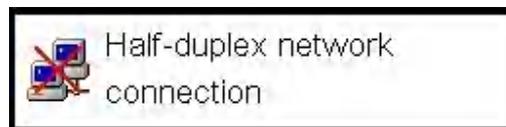


図 3-22 : Half Duplex オーバーレイ

3.14.3 Network Connection Lost オーバーレイ

ネットワーク接続の消失は、最新のスクリーンデータ経由の「Network connection lost」というメッセージを含むオーバーレイを使用して示されます。このオーバーレイは、クライアントネットワークケーブルが外された場合、または、クライアントで PCoIP プロトコルトラフィックが 2 秒以上受信されなかった場合に表示されます。



図 3-23 : Network Connection Lost オーバーレイ

このネットワーク接続消失メッセージは、ネットワークが回復するか、タイムアウトが切れる（および PCoIP セッションが終了する）まで表示されます。

注意：仮想デスクトップを備えた PCoIP デバイスを使用している場合は、この通知メッセージの使用はお勧めできません。仮想デスクトップハイパーバイザ内部の通常のスケジューリングによってこのメッセージが誤ってトリガーされる場合があります。この問題を回避するには、[Enable Peer Loss Overlay](#) 設定を無効にする必要があります。

3.14.4 No Support Resolutions Found

このオーバーレイは Tera2 クライアント上にもみ表示されます。ディスプレイの解像度は、4 つすべてのポートに大型のディスプレイが接続されている場合にリソース制約の影響を受ける可能性があります。解像度の制限を超えると、「No support resolutions found. Please try unplugging other displays.」というメッセージを含む以下のオーバーレイが表示されます。

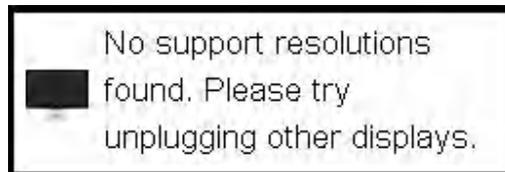


図 3-24 : No Support Resolutions Found オーバーレイ

3.14.5 Preparing Desktop オーバーレイ

始めて PCoIP セッションにログインしたときに、「Preparing desktop」というメッセージを含む以下のオーバーレイが表示されます。



図 3-25 : Preparing Desktop オーバーレイ

3.14.6 USB Device Not Authorized オーバーレイ

非許可 USB デバイスが接続された場合は、「USB device not authorized」というメッセージを含む以下のオーバーレイが表示されます。このオーバーレイは約 5 秒間表示されます。



図 3-26 : USB Device Not Authorized オーバーレイ

3.14.7 USB Over Current Notice オーバーレイ

クライアントに接続された USB デバイスを USB ポートで処理できない場合は、「USB over current notice」というメッセージを含む以下のオーバーレイが表示されます。このオーバーレイは、USB デバイスが取り除かれ、現在の USB ポートの処理が解消されるまで表示されます。

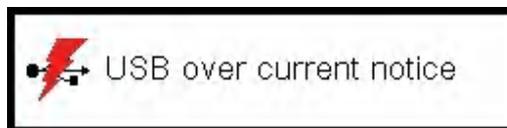


図 3-27 : USB Over Current Notice オーバーレイ

3.14.8 USB Device Not Supported Behind a High-speed Hub オーバーレイ

USB デバイスによってはハイスピード (USB 2.0) ハブ経由で接続できないものがあるため、その場合は、ゼロクライアントに直接接続するか、フルスピード (USB 1.1) ハブ経由で接続する必要があります。このようなデバイスがハイスピードハブ経由でゼロクライアントに接続されている場合は、「USB device not supported behind high speed hub」というメッセージを含む以下のオーバーレイが表示されます。このオーバーレイは約 5 秒間表示されます。

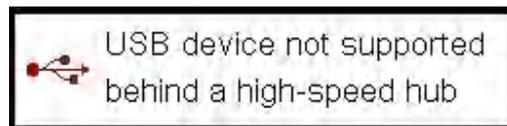


図 3-28 : USB Device Not Supported Behind a High-speed Hub オーバーレイ

3.14.9 Resolution Not Supported オーバーレイ

クライアントに接続されたモニタの解像度がホストでサポートできない場合は、モニタがデフォルト解像度に設定され、「Resolution not supported」というメッセージを含む以下のオーバーレイが表示されます。



図 3-29 : Resolution Not Supported オーバーレイ

3.14.10 Video Source オーバーレイ

不適切なホストビデオソースの接続は2つのオーバーレイで示される可能性があります。これらのオーバーレイは約5分間表示されます。モニタは、オーバーレイが表示されてから約15秒でスリープモードに入ります。

- ホストにビデオソースが接続されていない場合は、「No source signal」というメッセージを含む以下のオーバーレイが表示されます。これは、ホストにビデオソースが接続されていない状況やホスト PC がビデオ信号の駆動を停止していた状況をデバッグするのに役立ちます。これを修正するには、ホスト PC ビデオをホストに接続します（このメッセージは、ホストがディスプレイ電源セーブモードに入ったときにもトリガーされる可能性があります）。



図 3-30 : No Source Signal オーバーレイ

- ホストへのビデオソースがクライアント上で使用されているビデオポートに対応していない場合は、「Source signal on other port」というメッセージを含む以下のオーバーレイが表示されます。これは、ビデオソースが間違ったポートに接続されている状況をデバッグするのに役立ちます。これを修正するには、ホストまたはクライアントでビデオポートを交換します。

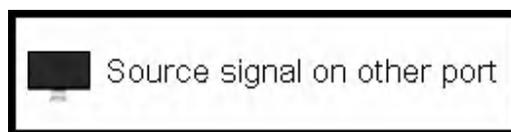


図 3-31 : Source Signal on Other Port オーバーレイ

3.15 OSD メニュー

画面左上の **Options** メニューには、OSD 設定ページ、情報ページ、およびステータスページにリンクされた5つのサブメニューがあります。

- **Configuration** : このメニューには、デバイスの動作と環境との相互作用を定義可能なページへのリンクが含まれています。各タブには、加えられた設定変更を受け入れたり、キャンセルしたりするための **OK**、**Cancel**、および **Apply** の各ボタンがあります。
- **Diagnostics** : このメニューには、クライアントに関する問題の診断を支援するページへのリンクが含まれています。
- **Information** : このメニュー下のページには、デバイスに関するハードウェアとファームウェアのバージョン情報が表示されます。

- **User Settings** : このメニューには、マウス、キーボード、イメージ、ディスプレイ、およびタッチスクリーンの設定と VMware View 証明書チェックモードを定義するためのページへのリンクが含まれています。
- **Password** : このメニュー下のページで、デバイスの管理パスワードを更新することができます。

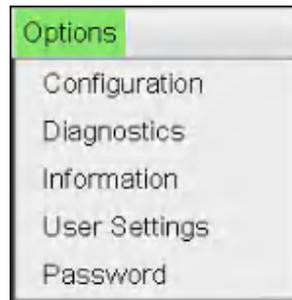


図 3-32 : OSD Options メニュー

注意：単一のメニュー項目、**Options** メニュー全体、またはすべてのメニューを非表示にすることができます。詳細については、「[MC : OSD 設定](#)」を参照してください。

このヘルプシステムの GUI リファレンスに各ページの詳細が記載されています。これらの OSD ページを使用してデバイスを設定または管理する方法については、GUI リファレンス内の該当するセクションを参照してください。

4 PCoIP デプロイメントシナリオ

4.1 PCoIP ホストカードとゼロクライアント

下の表は、PCoIP ネットワークにデプロイ可能な PCoIP ホストカードとゼロクライアントの一覧です。デバイスサポートごとのディスプレイ解像度のセットも含まれています。

注意：プロセッサ名は PCoIP デバイス内で使用されているチップセットを表しています。例えば、TERA2140 は第 2 世代 TERA2140 ゼロクライアントで使用されているプロセッサであり、TERA2240 は第 2 世代 TERA2240 PCIe ホストカード（タワー PC またはラックマウントワークステーション用）と TERA2240 PCI Mezzanine ホストカード（ブレードワークステーション用）で使用されているプロセッサです。

Teradici PCoIP プロセッサの詳細については、<http://www.teradici.com> にある Teradici ウェブサイトを参照してください。

任意のホストカードと任意のゼロクライアントを組み合わせることができます。ただし、ゼロクライアントをホストカードに接続する場合は、クライアントに接続されたディスプレイの最大サポート解像度が 2 つのデバイス間の最も一般的な基準に合わせられます。例えば、TERA2140 ゼロクライアントを TERA2240 ホストカードに接続する場合は、最大 4 台の 1920x1200 ディスプレイまたは 2 台の 2560x1600 ディスプレイを接続することができます。ただし、TERA2321 ゼロクライアントを同じホストカードに接続する場合は、選択肢が最大 2 台の 1920x1200 ディスプレイか、1 台の 2560x1600 ディスプレイになります。

表 4-1：PCoIP ホストカードとゼロクライアントのサポート解像度

プロセッサ名	サポート解像度の最大数	デバイスタイプ	プロセッサファミリー
TERA1100	2 x 1920x1200	ゼロクライアント	Tera1
TERA2321	2 x 1920x1200 1 x 2560x1600*	ゼロクライアント	Tera2
TERA2140	4 x 1920x1200 2 x 2560x1600*	ゼロクライアント	Tera2
TERA1202	2 x 1920x1200	ホストカード	Tera1
TERA2220	2 x 1920x1200 1 x 2560x1600	ホストカード	Tera2
TERA2240	4 x 1920x1200	ホストカード	Tera2

プロセッサ名	サポート解像度の最大数	デバイスタイプ	プロセッサファミリー
	2 x 2560x1600		

*Tera2 ゼロクライアントは、DVI インターフェースまたは DisplayPort インターフェースを使用して接続されたディスプレイ上で 2560x1600 解像度をサポートします。この解像度をサポートするための DVI ポートまたは DisplayPort ポートを使用した Tera2 ゼロクライアントへのケーブルの接続方法については、「[DVI インターフェースと DisplayPort インターフェース](#)」を参照してください。

4.1.1 プロセッサ情報の表示

ホストまたはクライアントの [AWI Home ページ](#) 上の **Processor** フィールドには、デバイスのプロセッサまたはチップセットの名前が表示されます。



Log Out PCoIP® Zero Client

Home Configuration / Permissions / Diagnostics / Info / Upload

PCoIP® Zero Client

PCoIP® device status and statistics for the current session.

Processor: TERA2140 Revision 1.0 (512 MB)
 Time Since Boot: 0 Days 16 Hours 37 Minutes 53 Seconds
 PCoIP Device Name: pcoip-portal-0030040ddbcb

Connection State: Connected to host [192.168.65.103](#)
 802.1X Authentication Status: Disabled
 Session Encryption Type: AES-256-GCM

PCoIP Packets (Sent/Received/Lost): 34716 / 52805 / 0
 Bytes (Sent/Received): 4401736 / 24021386
 Round Trip Latency (Min/Avg/Max): 2 / 2 / 4 ms
 Transmit Bandwidth (Min/Avg/Max/Limit): 8 / 120 / 392 / 8000 kbps
 Receive Bandwidth (Min/Avg/Max): 0 / 256 / 5600 kbps

Pipeline Processing Rate (Avg/Max/Limit): 1 / 37 / 297 Mpps
 Endpoint Image Settings In Use: Client
 Initial Image Quality (Min/Max): 40 / 90
 Image Quality Preference: 50
 Build To Lossless: Enabled

Display	Maximum Rate: Refresh Rate	Output Process Rate	Image Quality
1	60 fps	11 fps	Lossy
2	60 fps	0 fps	Lossless
3	N/A	N/A	N/A
4	N/A	N/A	N/A

図 4-1 : AWI Home ページ上のプロセッサ情報

プロセッサファミリ名はホストまたはクライアントの [AWI Version ページ](#) に表示されます。

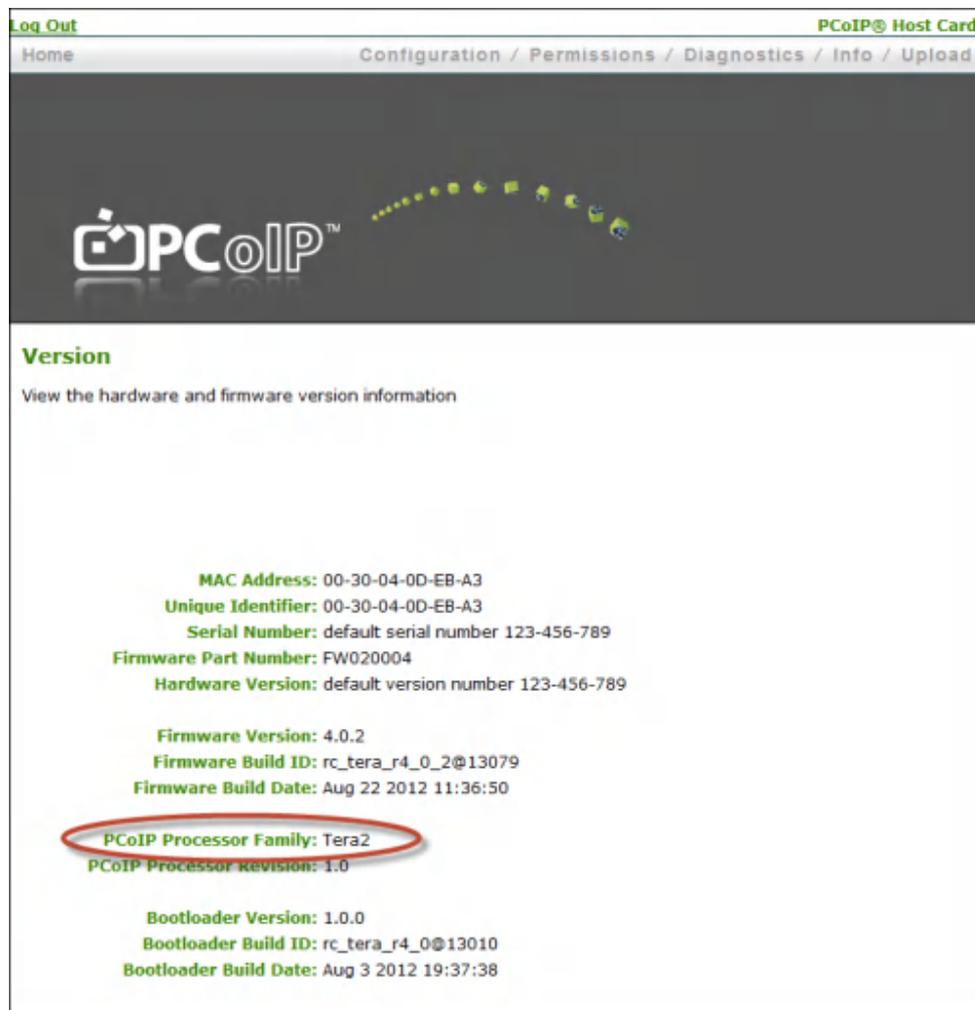


図 4-2 : AWI Version ページ上のプロセッサファミリ情報

デバイスの [OSD Version ページ](#) にゼロクライアントのプロセッサファミリ名を表示することもできます。

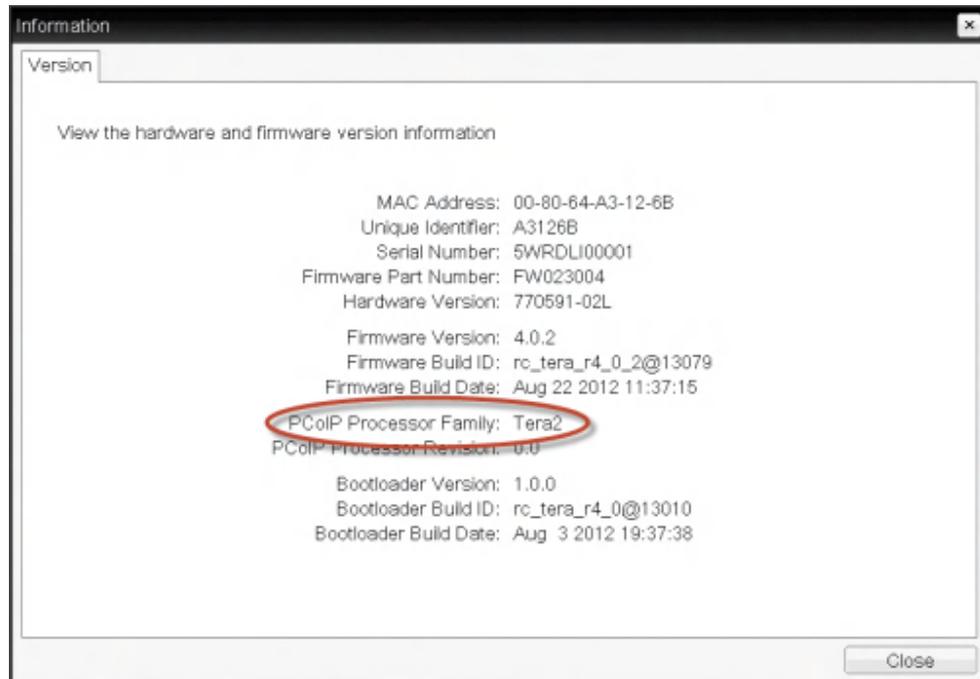


図 4-3 : OSD Version ページ上のプロセッサファミリー情報

4.2 TERA1100 ゼロクライアントと TERA1202 ホストカードの接続

このトピックでは、第 1 世代 TERA1100 ゼロクライアントと第 1 世代 TERA1202 ホストカード間の接続の設定方法について説明します。

注意：使用されているホストカードとゼロクライアントを特定するには、「[プロセッサ情報の表示](#)」を参照してください。クライアントとホストのディスプレイオプションを確認するには、「[PCoIP ホストカードとゼロクライアント](#)」を参照してください。

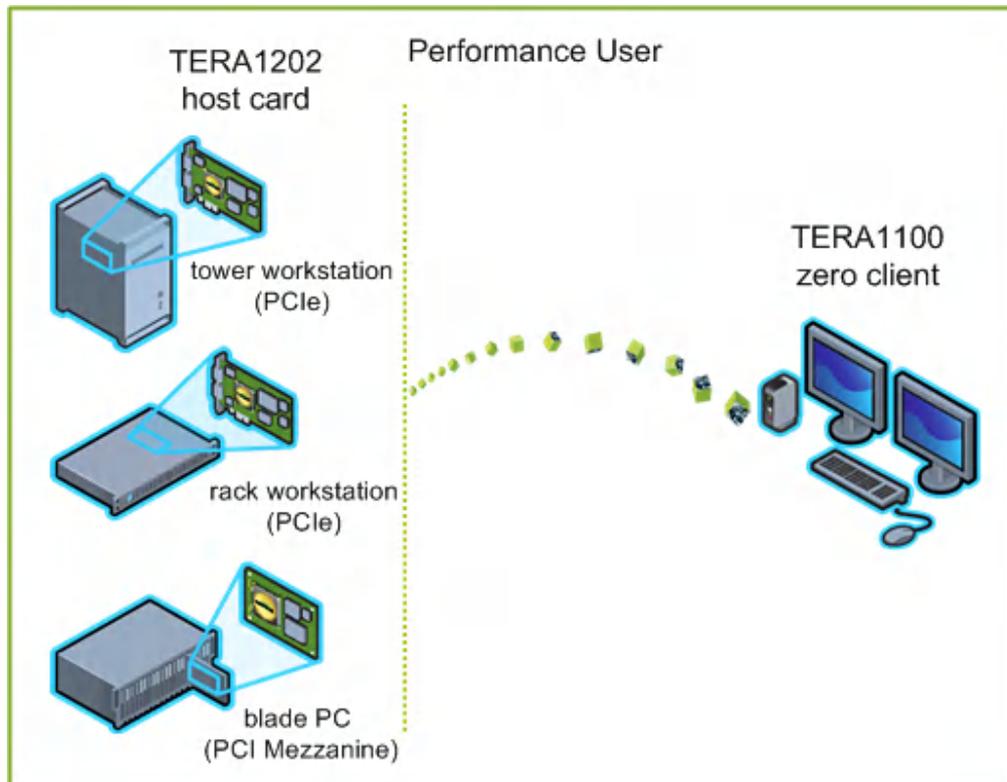


図 4-4 : TERA1100 ゼロクライアントと TERA1202 ホストカードの接続

図の左側は、タワーワークステーション、ラックワークステーション、ブレードワークステーションなどのホストカードをインストール可能なリモートワークステーションに関するフォームファクタを示しています。右側のゼロクライアントは、SLP ディスカバリ、VMware View Connection Server ブローカ、または別のサードパーティ製コネクションブローカを経由する直接ホスト/クライアント割り当てを通してリモートワークステーションに接続することができます。これらの接続オプションについては後述します。

注意：その他のクライアントオプションには、PCoIP 対応ディスプレイ、電話機、ラップトップ、iPad、およびその他の PCoIP 対応モバイルプラットフォームが含まれます。

4.3 前提条件

ホストカードとゼロクライアントを接続する前に、以下の条件を満たす必要があります。

- ホストカードとゼロクライアントのファームウェアバージョンを一致させる必要があります。MC を使用したファームウェアのアップロード方法については、『PCoIP Management Console User Manual』（TER0812002）を参照してください。MC を使用したプロファイルへのファームウェアファイルの割り当て方法については、「[MC：ファームウェア管理](#)」を参照してください。AWI を使用した単一

ホストまたはクライアントへのファームウェアのアップロード方法については、「[AWI: ファームウェアアップロード設定](#)」を参照してください。

- ネットワークリソースは、帯域幅、QoS、遅延、ジッタ、およびパケットロスに関する要件を満たすことができる必要があります。PCoIP ネットワークアーキテクチャの設計方法については、『[PC-over-IP Protocol Virtual Desktop Network Design Checklist](#)』（TER1105004）を参照してください。

4.3.1 セッション接続タイプ

PCoIP デプロイメントの規模によっては、管理コンソールまたはコネクションブローカを使用してホストカードとゼロクライアント間の接続を管理したり、AWI を使用して個々のホストとクライアントを、直接セッション接続タイプを使用するように設定したりすることができます。

注意：OSD を使用してセッション接続タイプ構成のクライアント側を設定することもできます。

次の 4 つの接続オプションが使用できます。

- [ホストとクライアントの静的な接続](#)
- [SLP ホストディスカバリを使用したホストとクライアントの接続](#)
- [サードパーティ製コネクションブローカを使用したホストとクライアントの接続](#)
- [VMware View Connection Server ブローカを使用したホストとクライアントの接続](#)

4.3.2 ホストとクライアントの静的な接続

クライアントを特定のホストカードに直接接続するように静的に設定するには、**Direct to Host** セッション接続タイプを使用します。このオプションの場合は、ホストの IP アドレス（または DNS 名）を指定する必要があります。

ホスト上で **Direct from Client** セッション接続タイプを設定する必要もあります。ホストが任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるようにするためのオプションがあります。後者の場合は、クライアントの MAC アドレスを指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Direct to Host](#) : MC を使用して、クライアントデバイスの **Direct to Host** セッション接続タイプを定義したプロファイルを設定する方法について説明します。MC を使用した特定のホストとクライアントの静的なリンク方法については、『[PCoIP Management Console User Manual](#)』（TER0812002）を参照してください。
- [AWI クライアント : Direct to Host](#) : AWI を使用して、クライアントを特定のホストカードに静的に接続するための設定方法について説明します。
- [AWI ホスト : Direct from Client](#) : AWI を使用して、ホストカードを任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるように設定する方法について説明します。

4.3.3 SLP ホストディスカバリを使用したホストとクライアントの接続

ホストがクライアントと同じネットワークサブネット上に存在する場合は、**Direct to Host + SLP** セッション接続タイプを使用して、クライアントがサービスロケーションプロトコル (SLP) を使用してサブネット上のホストを検出するように設定することができます。この設定では、クライアント OSD に、発見された最初の 10 ホストが一覧表示されます。必要なホストを選択してそれに接続することができます。

注意： SLP ホストディスカバリは、ホストが 10 を超える大規模なデプロイメントでクライアントがいずれかのホストに接続しなければならない場合には適していません。この場合は、[サードパーティ製コネクションブローカ](#)が必要です。

ホスト上で **Direct from Client** セッション接続タイプを設定する必要もあります。ホストが任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるようにするためのオプションがあります。後者の場合は、クライアントの MAC アドレスを指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Direct to Host + SLP](#) : MC を使用して、クライアントデバイスの **Direct to Host + SLP** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : Direct to Host + SLP](#) : AWI を使用して、クライアントを SLP ディスカバリ経由でホストカードに接続するための設定方法について説明します。
- [AWI ホスト : Direct from Client](#) : AWI を使用して、ホストカードを任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるように設定する方法について説明します。
- [OSD : Direct to Host + SLP](#) : OSD を使用して、クライアントを SLP ディスカバリ経由でホストカードに接続するための設定方法について説明します。

4.3.4 サードパーティ製コネクションブローカを使用したホストとクライアントの接続

サードパーティ製コネクションブローカは、ゼロクライアントから接続を確立しているユーザの ID に基づいて動的にホスト PC をゼロクライアントに割り当てるリソースマネージャです。コネクションブローカはホストのプールをゼロクライアントのグループに割り当てるためにも使用されます。コネクションブローカの多くは、大規模な PCoIP デプロイメントやホストとクライアントが同じサブネット上に存在しない環境で使用されます。

このオプションの場合は、ホストとクライアントの両方で **Connection Management Interface** セッション接続タイプを使用します。サードパーティ製コネクションブローカの IP アドレス (または DNS 名) を指定する必要があります。

注意： サードパーティ製コネクションブローカの詳細については、[Teradici サポートサイト](#)で知識ベースサポートトピック 15134-24 を参照してください。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Connection Management Interface](#) : MC を使用して、クライアントデバイスとホストデバイスの **Connection Management Interface** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : Connection Management Interface](#) : AWI を使用して、クライアントをサードパーティ製コネクションブローカ経由でクライアントとホスト間の接続を仲介するように設定する方法について説明します。
- [AWI ホスト : Connection Management Interface](#) : AWI を使用して、ホストをサードパーティ製コネクションブローカ経由でクライアントからの接続要求を受け入れるように設定する方法について説明します。
- [OSD : Connection Management Interface](#) : OSD を使用して、クライアントをサードパーティ製コネクションブローカ経由でクライアントとホスト間の接続を仲介するように設定する方法について説明します。

4.3.5 VMware View Connection Server ブローカを使用したホストとクライアントの接続

VMware View Connection Server ブローカを使用してクライアントとホストカード間の接続を仲介することもできます。

注意 : これは、ゼロクライアントを VMware View 仮想デスクトップに接続するための設定方法と同じではありません。

このオプションの場合は、VMware View Agent をホストワークステーションにインストールして、クライアントとホストの両方に関するその他のさまざまな設定要件をクリアする必要があります。詳細については、『Using PCoIP Host Cards with VMware View』（TER0911004）を参照してください。

4.3.6 その他の設定リンク

このセッションタイプに関するすべての範囲のファームウェアパラメータを設定するには、以下のトピックを参照してください。

注意 : OSD では一部の設定機能が使用できません。

MC を使用している場合	AWI を使用している場合	OSD を使用している場合
	AWI ホスト : 初期セットアップ AWI クライアント : 初期セットアップ	
MC : ネットワーク設定	AWI : ネットワーク設定	OSD : ネットワーク設定
MC を使用したデバイスネーミ	AWI : ラベル設定	OSD : ラベル設定

<p>ングの管理方法については、 『PCoIP Management Console User Manual』 (TER0812002) を参照してく ださい。</p>		
<p>MC : ディスカバリ設定</p>	<p>AWI : ディスカバリ設定</p>	<p>OSD : ディスカバリ設定</p>
<p>MC : SNMP 設定</p>	<p>AWI : SNMP 設定</p>	
<p>MC : Direct to Host MC : Direct to Host + SLP ホス トディスカバリ MC : Connection Management Interface</p>	<p>AWI ホスト : Direct from Client AWI クライアント : Direct to Host AWI クライアント : Direct to Host + SLP ホストディスカバ リ AWI ホスト : Connection Management Interface AWI クライアント : Connection Management Interface</p>	<p>OSD : Direct to Host OSD : Direct to Host + SLP ホ ストディスカバリ OSD : Connection Management Interface</p>
<p>MC : 暗号化設定</p>	<p>AWI : 暗号化設定</p>	
<p>MC : 帯域幅設定</p>	<p>AWI : 帯域幅設定</p>	
<p>MC : 言語設定</p>	<p>AWI クライアント : 言語設定</p>	<p>OSD : 言語設定</p>
<p>MC : OSD 設定</p>	<p>AWI : OSD 設定</p>	<p>OSD : OSD 設定</p>
<p>MC : イメージ設定</p>	<p>AWI ホスト : イメージ設定 AWI クライアント : イメージ設 定</p>	<p>OSD : イメージ設定</p>
<p>MC : モニタエミュレーション</p>	<p>AWI Tera1 ホスト : モニタエミ ュレーション</p>	
<p>MC : 時間設定</p>	<p>AWI : 時間設定</p>	
<p>MC : セキュリティ設定</p>	<p>AWI : セキュリティ設定</p>	
<p>MC : オーディオ承認</p>	<p>AWI ホスト : オーディオ承認 AWI クライアント : オーディオ 承認</p>	

MC : 電源承認	AWI クライアント : 電源承認	
MC : ホストドライバ機能	AWI ホスト : ホストドライバ機能	
MC : イベントログ設定	AWI : イベントログ設定	OSD : イベントログ設定
MC : 周辺機器設定	AWI クライアント : 周辺機器設定	
MC : IPv6 設定	AWI : IPv6 設定	OSD : IPv6 設定
MC : ディスプレイトポロジ設定		OSD Tera1 : ディスプレイトポロジ設定
MC : OSD ログ設定	AWI クライアント : OSD ログ設定	
MC : フォームウェア管理	AWI : フォームウェアアップロード設定	
MC : USB 承認	AWI ホスト : USB 承認 AWI クライアント : USB 承認	
MC : 証明書ストア管理	AWI : 証明書アップロード設定	
MC : VMware View 証明書チェック設定	AWI : VMware View 証明書チェック設定	OSD : VMware View 証明書チェック設定

4.4 TERA2321 ゼロクライアントと TERA1202 ホストカードの接続

このトピックでは、第2世代 TERA2321 ゼロクライアントと第1世代 TERA1202 ホストカード間の接続の設定方法について説明します。

注意：使用されているホストカードとゼロクライアントを特定するには、「[プロセッサ情報の表示](#)」を参照してください。クライアントとホストのディスプレイオプションを確認するには、「[PCoIP ホストカードとゼロクライアント](#)」を参照してください。

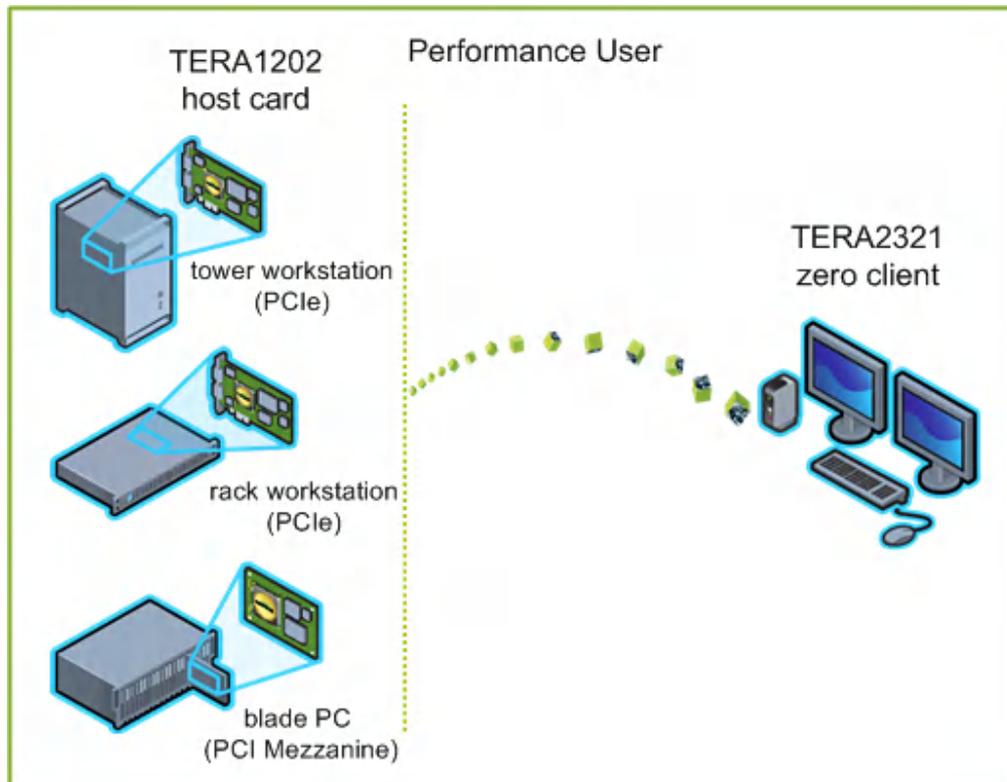


図 4-5 : TERA2321 ゼロクライアントと TERA1202 ホストカードの接続

図の左側は、タワーワークステーション、ラックワークステーション、ブレードワークステーションなどのホストカードをインストール可能なリモートワークステーションに関するフォームファクタを示しています。右側のゼロクライアントは、SLP ディスカバリ、VMware View Connection Server ブローカ、または別のサードパーティ製コネクションブローカを経由する直接ホスト/クライアント割り当てを通してリモートワークステーションに接続することができます。これらの接続オプションについては後述します。

注意：その他のクライアントオプションには、PCoIP 対応ディスプレイ、電話機、ラップトップ、iPad、およびその他の PCoIP 対応モバイルプラットフォームが含まれます。

4.5 前提条件

ホストカードとゼロクライアントを接続する前に、以下の条件を満たす必要があります。

- ホストカードとゼロクライアントのファームウェアバージョンを一致させる必要があります。MC を使用したファームウェアのアップロード方法については、『PCoIP Management Console User Manual』（TER0812002）を参照してください。MC を使用したプロファイルへのファームウェアファイルの割り当て方法については、「[MC：ファームウェア管理](#)」を参照してください。AWI を使用した単一

ホストまたはクライアントへのファームウェアのアップロード方法については、
「[AWI: ファームウェアアップロード設定](#)」を参照してください。

- ネットワークリソースは、帯域幅、QoS、遅延、ジッタ、およびパケットロスに関する要件を満たすことができる必要があります。PCoIP ネットワークアーキテクチャの設計方法については、『[PC-over-IP Protocol Virtual Desktop Network Design Checklist](#)』（TER1105004）を参照してください。

4.5.1 セッション接続タイプ

PCoIP デプロイメントの規模によっては、管理コンソールまたは接続ブローカを使用してホストカードとゼロクライアント間の接続を管理したり、AWI を使用して個々のホストとクライアントを直接セッション接続タイプを使用するように設定したりすることができます。

注意：OSD を使用してセッション接続タイプ構成のクライアント側を設定することもできます。

次の 4 つの接続オプションが使用できます。

- [ホストとクライアントの静的な接続](#)
- [SLP ホストディスカバリを使用したホストとクライアントの接続](#)
- [サードパーティ製接続ブローカを使用したホストとクライアントの接続](#)
- [VMware View Connection Server ブローカを使用したホストとクライアントの接続](#)

4.5.2 ホストとクライアントの静的な接続

クライアントを特定のホストカードに直接接続するように静的に設定するには、**Direct to Host** セッション接続タイプを使用します。このオプションの場合は、ホストの IP アドレス（または DNS 名）を指定する必要があります。

ホスト上で **Direct from Client** セッション接続タイプを設定する必要もあります。ホストが任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるようにするためのオプションがあります。後者の場合は、クライアントの MAC アドレスを指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Direct to Host](#) : MC を使用して、クライアントデバイスの **Direct to Host** セッション接続タイプを定義したプロファイルを設定する方法について説明します。MC を使用した特定のホストとクライアントの静的なリンク方法については、『[PCoIP Management Console User Manual](#)』（TER0812002）を参照してください。
- [AWI クライアント : Direct to Host](#) : AWI を使用して、クライアントを特定のホストカードに静的に接続するための設定方法について説明します。
- [AWI ホスト : Direct from Client](#) : AWI を使用して、ホストカードを任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるように設定する方法について説明します。

4.5.3 SLP ホストディスカバリを使用したホストとクライアントの接続

ホストがクライアントと同じネットワークサブネット上に存在する場合は、**Direct to Host + SLP** セッション接続タイプを使用して、クライアントがサービスロケーションプロトコル (SLP) を使用してサブネット上のホストを検出するように設定することができます。この設定では、クライアント OSD に、発見された最初の 10 ホストが一覧表示されます。必要なホストを選択してそれに接続することができます。

注意： SLP ホストディスカバリは、ホストが 10 を超える大規模なデプロイメントでクライアントがいずれかのホストに接続しなければならない場合には適していません。この場合は、[サードパーティ製コネクションブローカ](#)が必要です。

ホスト上で **Direct from Client** セッション接続タイプを設定する必要もあります。ホストが任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるようにするためのオプションがあります。後者の場合は、クライアントの MAC アドレスを指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Direct to Host + SLP](#) : MC を使用して、クライアントデバイスの **Direct to Host + SLP** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : Direct to Host + SLP](#) : AWI を使用して、クライアントを SLP ディスカバリ経由でホストカードに接続するための設定方法について説明します。
- [AWI ホスト : Direct from Client](#) : AWI を使用して、ホストカードを任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるように設定する方法について説明します。
- [OSD : Direct to Host + SLP](#) : OSD を使用して、クライアントを SLP ディスカバリ経由でホストカードに接続するための設定方法について説明します。

4.5.4 サードパーティ製コネクションブローカを使用したホストとクライアントの接続

サードパーティ製コネクションブローカは、ゼロクライアントから接続を確立しているユーザの ID に基づいて動的にホスト PC をゼロクライアントに割り当てるリソースマネージャです。コネクションブローカはホストのプールをゼロクライアントのグループに割り当てるためにも使用されます。コネクションブローカの多くは、大規模な PCoIP デプロイメントやホストとクライアントが同じサブネット上に存在しない環境で使用されます。

このオプションの場合は、ホストとクライアントの両方で **Connection Management Interface** セッション接続タイプを使用します。サードパーティ製コネクションブローカの IP アドレス (または DNS 名) を指定する必要があります。

注意： サードパーティ製コネクションブローカの詳細については、[Teradici サポートサイト](#)で知識ベースサポートトピック 15134-24 を参照してください。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Connection Management Interface](#) : MC を使用して、クライアントデバイスとホストデバイスの **Connection Management Interface** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : Connection Management Interface](#) : AWI を使用して、クライアントをサードパーティ製コネクションブローカ経由でクライアントとホスト間の接続を仲介するように設定する方法について説明します。
- [AWI ホスト : Connection Management Interface](#) : AWI を使用して、ホストをサードパーティ製コネクションブローカ経由でクライアントからの接続要求を受け入れるように設定する方法について説明します。
- [OSD : Connection Management Interface](#) : OSD を使用して、クライアントをサードパーティ製コネクションブローカ経由でクライアントとホスト間の接続を仲介するように設定する方法について説明します。

4.5.5 VMware View Connection Server ブローカを使用したホストとクライアントの接続

VMware View Connection Server ブローカを使用してクライアントとホストカード間の接続を仲介することもできます。

注意：これは、ゼロクライアントを VMware View 仮想デスクトップに接続するための設定方法と同じではありません。

このオプションの場合は、VMware View Agent をホストワークステーションにインストールして、クライアントとホストの両方に関するその他のさまざまな設定要件をクリアする必要があります。詳細については、『Using PCoIP Host Cards with VMware View』（TER0911004）を参照してください。

4.5.6 その他の設定リンク

このセッションタイプに関するすべての範囲のファームウェアパラメータを設定するには、以下のトピックを参照してください。

注意：OSD では一部の設定機能が使用できません。

注意：TERA2321 ゼロクライアントには第 1 世代 TERA1100 クライアントと同じディスプレイポロジがあります。このことは、このセクション内のディスプレイポロジページへのリンクに反映されています。

MC を使用している場合	AWI を使用している場合	OSD を使用している場合
	AWI ホスト : 初期セットアップ AWI クライアント : 初期セットアップ	

MC : ネットワーク設定	AWI : ネットワーク設定	OSD : ネットワーク設定
MCを使用したデバイスネーミングの管理方法については、『PCoIP Management Console User Manual』(TER0812002)を参照してください。	AWI : ラベル設定	OSD : ラベル設定
MC : ディスカバリ設定	AWI : ディスカバリ設定	OSD : ディスカバリ設定
MC : SNMP 設定	AWI : SNMP 設定	
MC : Direct to Host MC : Direct to Host + SLP ホストディスカバリ MC : Connection Management Interface	AWI ホスト : Direct from Client AWI クライアント : Direct to Host AWI クライアント : Direct to Host + SLP ホストディスカバリ AWI ホスト : Connection Management Interface AWI クライアント : Connection Management Interface	OSD : Direct to Host OSD : Direct to Host + SLP ホストディスカバリ OSD : Connection Management Interface
MC : 暗号化設定	AWI : 暗号化設定	
MC : 帯域幅設定	AWI : 帯域幅設定	
MC : 言語設定	AWI クライアント : 言語設定	OSD : 言語設定
MC : OSD 設定	AWI : OSD 設定	OSD : OSD 設定
MC : イメージ設定	AWI ホスト : イメージ設定 AWI クライアント : イメージ設定	OSD : イメージ設定
MC : モニタエミュレーション	AWI Tera1 ホスト : モニタエミュレーション	
MC : 時間設定	AWI : 時間設定	
MC : セキュリティ設定	AWI : セキュリティ設定	
MC : オーディオ承認	AWI ホスト : オーディオ承認	

	AWI クライアント : オーディオ承認	
MC : 電源承認	AWI クライアント : 電源承認	
MC : ホストドライバ機能	AWI ホスト : ホストドライバ機能	
MC : イベントログ設定	AWI : イベントログ設定	OSD : イベントログ設定
MC : 周辺機器設定	AWI クライアント : 周辺機器設定	
MC : IPv6 設定	AWI : IPv6 設定	OSD : IPv6 設定
MC : ディスプレイトポロジ設定		OSD Tera1 : ディスプレイトポロジ設定
MC : OSD ログ設定	AWI クライアント : OSD ログ設定	
MC : フォームウェア管理	AWI : ファームウェアアップロード設定	
MC : USB 承認	AWI ホスト : USB 承認 AWI クライアント : USB 承認	
MC : 証明書ストア管理	AWI : 証明書アップロード設定	
MC : VMware View 証明書チェック設定	AWI : VMware View 証明書チェック設定	OSD : VMware View 証明書チェック設定

4.6 TERA2140 ゼロクライアントと TERA1202 ホストカードの接続

このトピックでは、第2世代 TERA2140 ゼロクライアントと第1世代 TERA1202 ホストカード間の接続の設定方法について説明します。

注意：使用されているホストカードとゼロクライアントを特定するには、「[プロセッサ情報の表示](#)」を参照してください。クライアントとホストのディスプレイオプションを確認するには、「[PCoIP ホストカードとゼロクライアント](#)」を参照してください。

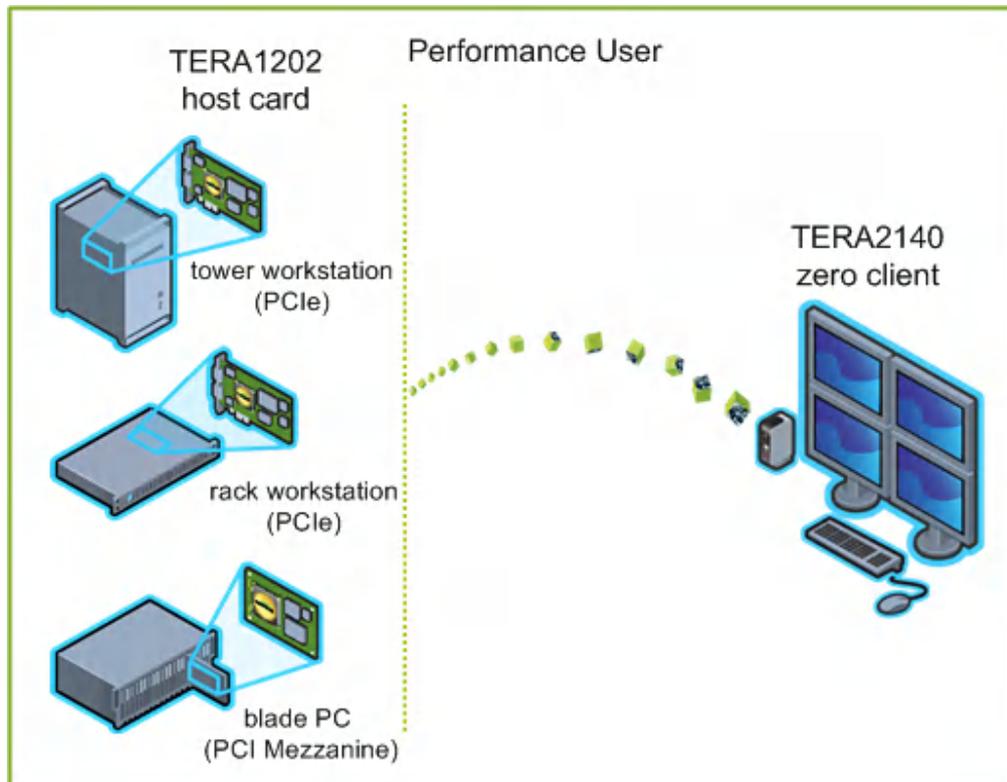


図 4-6 : TERA2140 ゼロクライアントと TERA1202 ホストカードの接続

図の左側は、タワーワークステーション、ラックワークステーション、ブレードワークステーションなどのホストカードをインストール可能なリモートワークステーションに関するフォームファクタを示しています。右側のゼロクライアントは、SLP ディスカバリ、VMware View Connection Server ブローカ、または別のサードパーティ製コネクションブローカを経由する直接ホスト/クライアント割り当てを通してリモートワークステーションに接続することができます。これらの接続オプションについては後述します。

注意：その他のクライアントオプションには、PCoIP 対応ディスプレイ、電話機、ラップトップ、iPad、およびその他の PCoIP 対応モバイルプラットフォームが含まれます。

4.7 前提条件

ホストカードとゼロクライアントを接続する前に、以下の条件を満たす必要があります。

- ホストカードとゼロクライアントのファームウェアバージョンを一致させる必要があります。MC を使用したファームウェアのアップロード方法については、『PCoIP Management Console User Manual』（TER0812002）を参照してください。MC を使用したプロファイルへのファームウェアファイルの割り当て方法については、「[MC：ファームウェア管理](#)」を参照してください。AWI を使用した単一

ホストまたはクライアントへのファームウェアのアップロード方法については、
「[AWI: ファームウェアアップロード設定](#)」を参照してください。

- ネットワークリソースは、帯域幅、QoS、遅延、ジッタ、およびパケットロスに関する要件を満たすことができる必要があります。PCoIP ネットワークアーキテクチャの設計方法については、『[PC-over-IP Protocol Virtual Desktop Network Design Checklist](#)』（TER1105004）を参照してください。

4.7.1 セッション接続タイプ

PCoIP デプロイメントの規模によっては、管理コンソールまたはコネクシオンブローカを使用してホストカードとゼロクライアント間の接続を管理したり、AWI を使用して個々のホストとクライアントを、直接セッション接続タイプを使用するように設定したりすることができます。

注意：OSD を使用してセッション接続タイプ構成のクライアント側を設定することもできます。

次の 4 つの接続オプションが使用できます。

- [ホストとクライアントの静的な接続](#)
- [SLP ホストディスカバリを使用したホストとクライアントの接続](#)
- [サードパーティ製コネクシオンブローカを使用したホストとクライアントの接続](#)
- [VMware View Connection Server ブローカを使用したホストとクライアントの接続](#)

4.7.2 ホストとクライアントの静的な接続

クライアントを特定のホストカードに直接接続するように静的に設定するには、**Direct to Host** セッション接続タイプを使用します。このオプションの場合は、ホストの IP アドレス（または DNS 名）を指定する必要があります。

ホスト上で **Direct from Client** セッション接続タイプを設定する必要もあります。ホストが任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるようにするためのオプションがあります。後者の場合は、クライアントの MAC アドレスを指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Direct to Host](#) : MC を使用して、クライアントデバイスの **Direct to Host** セッション接続タイプを定義したプロファイルを設定する方法について説明します。MC を使用した特定のホストとクライアントの静的なリンク方法については、『[PCoIP Management Console User Manual](#)』（TER0812002）を参照してください。
- [AWI クライアント : Direct to Host](#) : AWI を使用して、クライアントを特定のホストカードに静的に接続するための設定方法について説明します。
- [AWI ホスト : Direct from Client](#) : AWI を使用して、ホストカードを任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるように設定する方法について説明します。

4.7.3 SLP ホストディスカバリを使用したホストとクライアントの接続

ホストがクライアントと同じネットワークサブネット上に存在する場合は、**Direct to Host + SLP** セッション接続タイプを使用して、クライアントがサービスロケーションプロトコル (SLP) を使用してサブネット上のホストを検出するように設定することができます。この設定では、クライアント OSD に、発見された最初の 10 ホストが一覧表示されます。必要なホストを選択してそれに接続することができます。

注意： SLP ホストディスカバリは、ホストが 10 を超える大規模なデプロイメントでクライアントがいずれかのホストに接続しなければならない場合には適していません。この場合は、[サードパーティ製コネクションブローカ](#)が必要です。

ホスト上で **Direct from Client** セッション接続タイプを設定する必要もあります。ホストが任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるようにするためのオプションがあります。後者の場合は、クライアントの MAC アドレスを指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Direct to Host + SLP](#) : MC を使用して、クライアントデバイスの **Direct to Host + SLP** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : Direct to Host + SLP](#) : AWI を使用して、クライアントを SLP ディスカバリ経由でホストカードに接続するための設定方法について説明します。
- [AWI ホスト : Direct from Client](#) : AWI を使用して、ホストカードを任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるように設定する方法について説明します。
- [OSD : Direct to Host + SLP](#) : OSD を使用して、クライアントを SLP ディスカバリ経由でホストカードに接続するための設定方法について説明します。

4.7.4 サードパーティ製コネクションブローカを使用したホストとクライアントの接続

サードパーティ製コネクションブローカは、ゼロクライアントから接続を確立しているユーザの ID に基づいて動的にホスト PC をゼロクライアントに割り当てるリソースマネージャです。コネクションブローカはホストのプールをゼロクライアントのグループに割り当てるためにも使用されます。コネクションブローカの多くは、大規模な PCoIP デプロイメントやホストとクライアントが同じサブネット上に存在しない環境で使用されます。

このオプションの場合は、ホストとクライアントの両方で **Connection Management Interface** セッション接続タイプを使用します。サードパーティ製コネクションブローカの IP アドレス (または DNS 名) を指定する必要があります。

注意： サードパーティ製コネクションブローカの詳細については、[Teradici サポートサイト](#)で知識ベースサポートトピック 15134-24 を参照してください。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Connection Management Interface](#) : MC を使用して、クライアントデバイスとホストデバイスの **Connection Management Interface** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : Connection Management Interface](#) : AWI を使用して、クライアントをサードパーティ製コネクションブローカ経由でクライアントとホスト間の接続を仲介するように設定する方法について説明します。
- [AWI ホスト : Connection Management Interface](#) : AWI を使用して、ホストをサードパーティ製コネクションブローカ経由でクライアントからの接続要求を受け入れるように設定する方法について説明します。
- [OSD : Connection Management Interface](#) : OSD を使用して、クライアントをサードパーティ製コネクションブローカ経由でクライアントとホスト間の接続を仲介するように設定する方法について説明します。

4.7.5 VMware View Connection Server ブローカを使用したホストとクライアントの接続

VMware View Connection Server ブローカを使用してクライアントとホストカード間の接続を仲介することもできます。

注意：これは、ゼロクライアントを VMware View 仮想デスクトップに接続するための設定方法と同じではありません。

このオプションの場合は、VMware View Agent をホストワークステーションにインストールして、クライアントとホストの両方に関するその他のさまざまな設定要件をクリアする必要があります。詳細については、『Using PCoIP Host Cards with VMware View』（TER0911004）を参照してください。

4.7.6 その他の設定リンク

このセッションタイプに関するすべての範囲のファームウェアパラメータを設定するには、以下のトピックを参照してください。

注意：OSD では一部の設定機能が使用できません。

MC を使用している場合	AWI を使用している場合	OSD を使用している場合
	AWI ホスト : 初期セットアップ AWI クライアント : 初期セットアップ	
MC : ネットワーク設定	AWI : ネットワーク設定	OSD : ネットワーク設定
MC を使用したデバイスネーミ	AWI : ラベル設定	OSD : ラベル設定

<p>ングの管理方法については、 『PCoIP Management Console User Manual』 (TER0812002) を参照してく ださい。</p>		
<p>MC : ディスカバリ設定</p>	<p>AWI : ディスカバリ設定</p>	<p>OSD : ディスカバリ設定</p>
<p>MC : SNMP 設定</p>	<p>AWI : SNMP 設定</p>	
<p>MC : Direct to Host MC : Direct to Host + SLP ホス トディスカバリ MC : Connection Management Interface</p>	<p>AWI ホスト : Direct from Client AWI クライアント : Direct to Host AWI クライアント : Direct to Host + SLP ホストディスカバ リ AWI ホスト : Connection Management Interface AWI クライアント : Connection Management Interface</p>	<p>OSD : Direct to Host OSD : Direct to Host + SLP ホ ストディスカバリ OSD : Connection Management Interface</p>
<p>MC : 暗号化設定</p>	<p>AWI : 暗号化設定</p>	
<p>MC : 帯域幅設定</p>	<p>AWI : 帯域幅設定</p>	
<p>MC : 言語設定</p>	<p>AWI クライアント : 言語設定</p>	<p>OSD : 言語設定</p>
<p>MC : OSD 設定</p>	<p>AWI : OSD 設定</p>	<p>OSD : OSD 設定</p>
<p>MC : イメージ設定</p>	<p>AWI ホスト : イメージ設定 AWI クライアント : イメージ設 定</p>	<p>OSD : イメージ設定</p>
<p>MC : モニタエミュレーション</p>	<p>AWI Tera1 ホスト : モニタエミ ュレーション</p>	
<p>MC : 時間設定</p>	<p>AWI : 時間設定</p>	
<p>MC : セキュリティ設定</p>	<p>AWI : セキュリティ設定</p>	
<p>MC : オーディオ承認</p>	<p>AWI ホスト : オーディオ承認 AWI クライアント : オーディオ 承認</p>	

MC : 電源承認	AWI クライアント : 電源承認	
MC : ホストドライバ機能	AWI ホスト : ホストドライバ機能	
MC : イベントログ設定	AWI : イベントログ設定	OSD : イベントログ設定
MC : 周辺機器設定	AWI クライアント : 周辺機器設定	
MC : IPv6 設定	AWI : IPv6 設定	OSD : IPv6 設定
MC : ディスプレイトポロジ設定		OSD Tera2 : ディスプレイトポロジ設定
MC : OSD ログ設定	AWI クライアント : OSD ログ設定	
MC : フォームウェア管理	AWI : フォームウェアアップロード設定	
MC : USB 承認	AWI ホスト : USB 承認 AWI クライアント : USB 承認	
MC : 証明書ストア管理	AWI : 証明書アップロード設定	
MC : VMware View 証明書チェック設定	AWI : VMware View 証明書チェック設定	OSD : VMware View 証明書チェック設定

4.8 TERA1100 ゼロクライアントと TERA2220 ホストカードの接続

このトピックでは、第1世代 TERA1100 ゼロクライアントと第2世代 TERA2220 ホストカード間の接続の設定方法について説明します。

注意：使用されているホストカードとゼロクライアントを特定するには、「[プロセッサ情報の表示](#)」を参照してください。クライアントとホストのディスプレイオプションを確認するには、「[PCoIP ホストカードとゼロクライアント](#)」を参照してください。

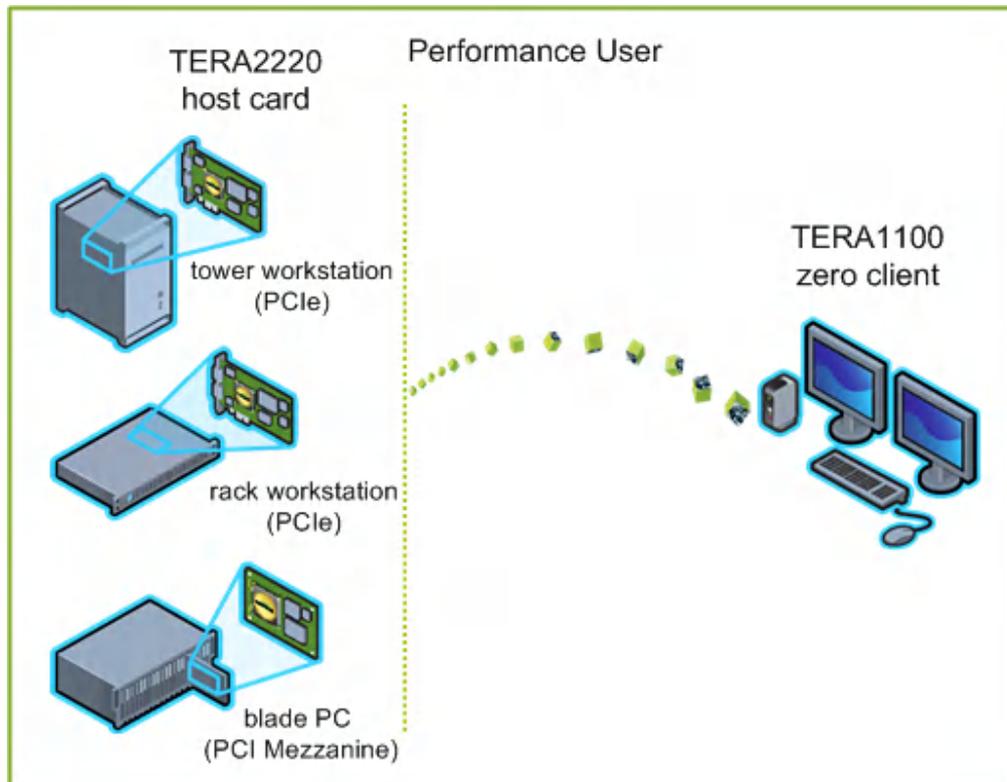


図 4-7 : TERA1100 ゼロクライアントと TERA2220 ホストカードの接続

図の左側は、タワーワークステーション、ラックワークステーション、ブレードワークステーションなどのホストカードをインストール可能なリモートワークステーションに関するフォームファクタを示しています。右側のゼロクライアントは、SLP ディスカバリ、VMware View Connection Server ブローカ、または別のサードパーティ製コネクショナルブローカを経由する直接ホスト/クライアント割り当てを通してリモートワークステーションに接続することができます。これらの接続オプションについては後述します。

注意：その他のクライアントオプションには、PCoIP 対応ディスプレイ、電話機、ラップトップ、iPad、およびその他の PCoIP 対応モバイルプラットフォームが含まれます。

4.9 前提条件

ホストカードとゼロクライアントを接続する前に、以下の条件を満たす必要があります。

- ホストカードとゼロクライアントのファームウェアバージョンを一致させる必要があります。MC を使用したファームウェアのアップロード方法については、『PCoIP Management Console User Manual』（TER0812002）を参照してください。MC を使用したプロファイルへのファームウェアファイルの割り当て方法については、「[MC：ファームウェア管理](#)」を参照してください。AWI を使用した単一

ホストまたはクライアントへのファームウェアのアップロード方法については、「[AWI: ファームウェアアップロード設定](#)」を参照してください。

- ネットワークリソースは、帯域幅、QoS、遅延、ジッタ、およびパケットロスに関する要件を満たすことができる必要があります。PCoIP ネットワークアーキテクチャの設計方法については、『[PC-over-IP Protocol Virtual Desktop Network Design Checklist](#)』（TER1105004）を参照してください。

4.9.1 セッション接続タイプ

PCoIP デプロイメントの規模によっては、管理コンソールまたは接続ブローカを使用してホストカードとゼロクライアント間の接続を管理したり、AWI を使用して個々のホストとクライアントを、直接セッション接続タイプを使用するように設定したりすることができます。

注意：OSD を使用してセッション接続タイプ構成のクライアント側を設定することもできます。

次の 4 つの接続オプションが使用できます。

- [ホストとクライアントの静的な接続](#)
- [SLP ホストディスカバリを使用したホストとクライアントの接続](#)
- [サードパーティ製接続ブローカを使用したホストとクライアントの接続](#)
- [VMware View Connection Server ブローカを使用したホストとクライアントの接続](#)

4.9.2 ホストとクライアントの静的な接続

クライアントを特定のホストカードに直接接続するように静的に設定するには、**Direct to Host** セッション接続タイプを使用します。このオプションの場合は、ホストの IP アドレス（または DNS 名）を指定する必要があります。

ホスト上で **Direct from Client** セッション接続タイプを設定する必要もあります。ホストが任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるようにするためのオプションがあります。後者の場合は、クライアントの MAC アドレスを指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Direct to Host](#) : MC を使用して、クライアントデバイスの **Direct to Host** セッション接続タイプを定義したプロファイルを設定する方法について説明します。MC を使用した特定のホストとクライアントの静的なリンク方法については、『[PCoIP Management Console User Manual](#)』（TER0812002）を参照してください。
- [AWI クライアント : Direct to Host](#) : AWI を使用して、クライアントを特定のホストカードに静的に接続するための設定方法について説明します。
- [AWI ホスト : Direct from Client](#) : AWI を使用して、ホストカードを任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるように設定する方法について説明します。

4.9.3 SLP ホストディスカバリを使用したホストとクライアントの接続

ホストがクライアントと同じネットワークサブネット上に存在する場合は、**Direct to Host + SLP** セッション接続タイプを使用して、クライアントがサービスロケーションプロトコル (SLP) を使用してサブネット上のホストを検出するように設定することができます。この設定では、クライアント OSD に、発見された最初の 10 ホストが一覧表示されます。必要なホストを選択してそれに接続することができます。

注意： SLP ホストディスカバリは、ホストが 10 を超える大規模なデプロイメントでクライアントがいずれかのホストに接続しなければならない場合には適していません。この場合は、[サードパーティ製コネクションブローカ](#)が必要です。

ホスト上で **Direct from Client** セッション接続タイプを設定する必要もあります。ホストが任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるようにするためのオプションがあります。後者の場合は、クライアントの MAC アドレスを指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Direct to Host + SLP](#) : MC を使用して、クライアントデバイスの **Direct to Host + SLP** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : Direct to Host + SLP](#) : AWI を使用して、クライアントを SLP ディスカバリ経由でホストカードに接続するための設定方法について説明します。
- [AWI ホスト : Direct from Client](#) : AWI を使用して、ホストカードを任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるように設定する方法について説明します。
- [OSD : Direct to Host + SLP](#) : OSD を使用して、クライアントを SLP ディスカバリ経由でホストカードに接続するための設定方法について説明します。

4.9.4 サードパーティ製コネクションブローカを使用したホストとクライアントの接続

サードパーティ製コネクションブローカは、ゼロクライアントから接続を確立しているユーザの ID に基づいて動的にホスト PC をゼロクライアントに割り当てるリソースマネージャです。コネクションブローカはホストのプールをゼロクライアントのグループに割り当てるためにも使用されます。コネクションブローカの多くは、大規模な PCoIP デプロイメントやホストとクライアントが同じサブネット上に存在しない環境で使用されます。

このオプションの場合は、ホストとクライアントの両方で **Connection Management Interface** セッション接続タイプを使用します。サードパーティ製コネクションブローカの IP アドレス (または DNS 名) を指定する必要があります。

注意： サードパーティ製コネクションブローカの詳細については、[Teradici サポートサイト](#)で知識ベースサポートトピック 15134-24 を参照してください。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Connection Management Interface](#) : MC を使用して、クライアントデバイスとホストデバイスの **Connection Management Interface** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : Connection Management Interface](#) : AWI を使用して、クライアントをサードパーティ製コネクションブローカ経由でクライアントとホスト間の接続を仲介するように設定する方法について説明します。
- [AWI ホスト : Connection Management Interface](#) : AWI を使用して、ホストをサードパーティ製コネクションブローカ経由でクライアントからの接続要求を受け入れるように設定する方法について説明します。
- [OSD : Connection Management Interface](#) : OSD を使用して、クライアントをサードパーティ製コネクションブローカ経由でクライアントとホスト間の接続を仲介するように設定する方法について説明します。

4.9.5 VMware View Connection Server ブローカを使用したホストとクライアントの接続

VMware View Connection Server ブローカを使用してクライアントとホストカード間の接続を仲介することもできます。

注意：これは、ゼロクライアントを VMware View 仮想デスクトップに接続するための設定方法と同じではありません。

このオプションの場合は、VMware View Agent をホストワークステーションにインストールして、クライアントとホストの両方に関するその他のさまざまな設定要件をクリアする必要があります。詳細については、『Using PCoIP Host Cards with VMware View』（TER0911004）を参照してください。

4.9.6 その他の設定リンク

このセッションタイプに関するすべての範囲のファームウェアパラメータを設定するには、以下のトピックを参照してください。

注意：OSD では一部の設定機能が使用できません。

MC を使用している場合	AWI を使用している場合	OSD を使用している場合
	AWI ホスト : 初期セットアップ AWI クライアント : 初期セットアップ	
MC : ネットワーク設定	AWI : ネットワーク設定	OSD : ネットワーク設定
MC を使用したデバイスネーミ	AWI : ラベル設定	OSD : ラベル設定

<p>ングの管理方法については、 『PCoIP Management Console User Manual』 (TER0812002) を参照してく ださい。</p>		
<p>MC : ディスカバリ設定</p>	<p>AWI : ディスカバリ設定</p>	<p>OSD : ディスカバリ設定</p>
<p>MC : SNMP 設定</p>	<p>AWI : SNMP 設定</p>	
<p>MC : Direct to Host MC : Direct to Host + SLP ホス トディスカバリ MC : Connection Management Interface</p>	<p>AWI ホスト : Direct from Client AWI クライアント : Direct to Host AWI クライアント : Direct to Host + SLP ホストディスカバ リ AWI ホスト : Connection Management Interface AWI クライアント : Connection Management Interface</p>	<p>OSD : Direct to Host OSD : Direct to Host + SLP ホ ストディスカバリ OSD : Connection Management Interface</p>
<p>MC : 暗号化設定</p>	<p>AWI : 暗号化設定</p>	
<p>MC : 帯域幅設定</p>	<p>AWI : 帯域幅設定</p>	
<p>MC : 言語設定</p>	<p>AWI クライアント : 言語設定</p>	<p>OSD : 言語設定</p>
<p>MC : OSD 設定</p>	<p>AWI : OSD 設定</p>	<p>OSD : OSD 設定</p>
<p>MC : イメージ設定</p>	<p>AWI ホスト : イメージ設定 AWI クライアント : イメージ設 定</p>	<p>OSD : イメージ設定</p>
<p>MC : モニタエミュレーション</p>	<p>AWI Tera2 ホスト : モニタエミ ュレーション</p>	
<p>MC : 時間設定</p>	<p>AWI : 時間設定</p>	
<p>MC : セキュリティ設定</p>	<p>AWI : セキュリティ設定</p>	
<p>MC : オーディオ承認</p>	<p>AWI ホスト : オーディオ承認 AWI クライアント : オーディオ 承認</p>	

MC : 電源承認	AWI クライアント : 電源承認	
MC : ホストドライバ機能	AWI ホスト : ホストドライバ機能	
MC : イベントログ設定	AWI : イベントログ設定	OSD : イベントログ設定
MC : 周辺機器設定	AWI クライアント : 周辺機器設定	
MC : IPv6 設定	AWI : IPv6 設定	OSD : IPv6 設定
MC : ディスプレイトポロジ設定		OSD Tera1 : ディスプレイトポロジ設定
MC : OSD ログ設定	AWI クライアント : OSD ログ設定	
MC : フォームウェア管理	AWI : フォームウェアアップロード設定	
MC : USB 承認	AWI ホスト : USB 承認 AWI クライアント : USB 承認	
MC : 証明書ストア管理	AWI : 証明書アップロード設定	
MC : VMware View 証明書チェック設定	AWI : VMware View 証明書チェック設定	OSD : VMware View 証明書チェック設定

4.10 TERA2321 ゼロクライアントと TERA2220 ホストカードの接続

このトピックでは、第2世代 TERA2321 ゼロクライアントと第2世代 TERA2220 ホストカード間の接続の設定方法について説明します。

注意：使用されているホストカードとゼロクライアントを特定するには、「[プロセス情報の表示](#)」を参照してください。クライアントとホストのディスプレイオプションを確認するには、「[PCoIP ホストカードとゼロクライアント](#)」を参照してください。

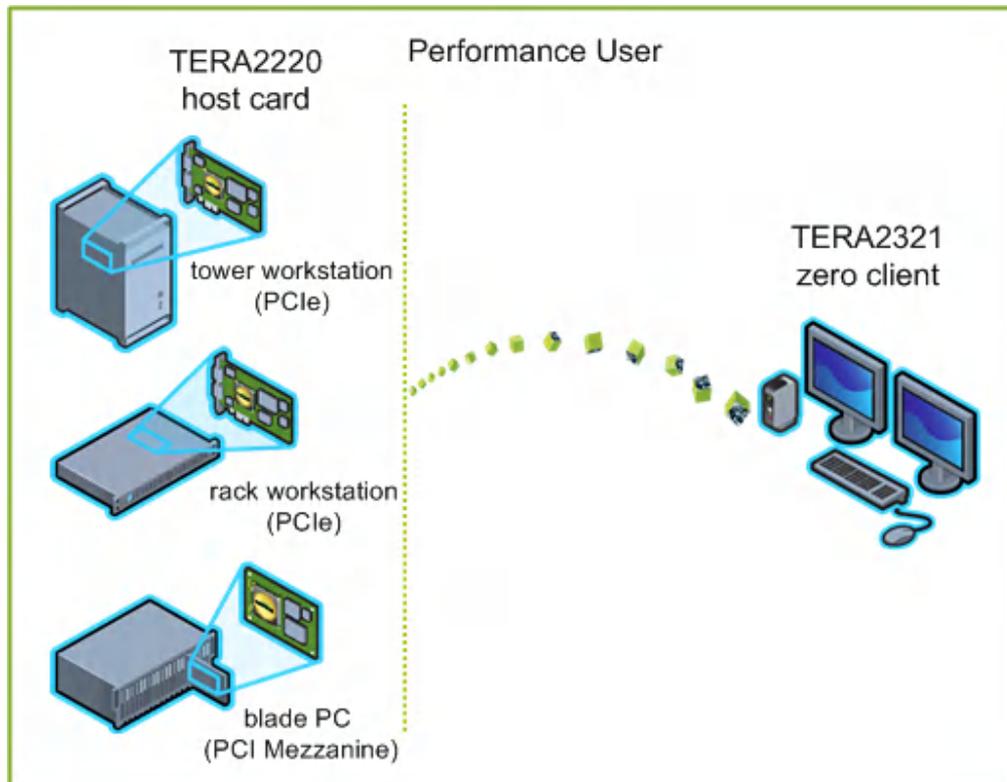


図 4-8 : TERA2321 ゼロクライアントと TERA2220 ホストカードの接続

図の左側は、タワーワークステーション、ラックワークステーション、ブレードワークステーションなどのホストカードをインストール可能なリモートワークステーションに関するフォームファクタを示しています。右側のゼロクライアントは、SLP ディスカバリ、VMware View Connection Server ブローカ、または別のサードパーティ製接続ブローカを経由する直接ホスト/クライアント割り当てを通してリモートワークステーションに接続することができます。これらの接続オプションについては後述します。

注意：その他のクライアントオプションには、PCoIP 対応ディスプレイ、電話機、ラップトップ、iPad、およびその他の PCoIP 対応モバイルプラットフォームが含まれます。

4.11 前提条件

ホストカードとゼロクライアントを接続する前に、以下の条件を満たす必要があります。

- ホストカードとゼロクライアントのファームウェアバージョンを一致させる必要があります。MC を使用したファームウェアのアップロード方法については、『PCoIP Management Console User Manual』（TER0812002）を参照してください。MC を使用したプロファイルへのファームウェアファイルの割り当て方法については、「[MC：ファームウェア管理](#)」を参照してください。AWI を使用した単一

ホストまたはクライアントへのファームウェアのアップロード方法については、
「[AWI: ファームウェアアップロード設定](#)」を参照してください。

- ネットワークリソースは、帯域幅、QoS、遅延、ジッタ、およびパケットロスに関する要件を満たすことができる必要があります。PCoIP ネットワークアーキテクチャの設計方法については、『PC-over-IP Protocol Virtual Desktop Network Design Checklist』（TER1105004）を参照してください。

4.11.1 セッション接続タイプ

PCoIP デプロイメントの規模によっては、管理コンソールまたはコネクシオンブローカを使用してホストカードとゼロクライアント間の接続を管理したり、AWI を使用して個々のホストとクライアントを、直接セッション接続タイプを使用するように設定したりすることができます。

注意：OSD を使用してセッション接続タイプ構成のクライアント側を設定することもできます。

次の 4 つの接続オプションが使用できます。

- [ホストとクライアントの静的な接続](#)
- [SLP ホストディスカバリを使用したホストとクライアントの接続](#)
- [サードパーティ製コネクシオンブローカを使用したホストとクライアントの接続](#)
- [VMware View Connection Server ブローカを使用したホストとクライアントの接続](#)

4.11.2 ホストとクライアントの静的な接続

クライアントを特定のホストカードに直接接続するように静的に設定するには、**Direct to Host** セッション接続タイプを使用します。このオプションの場合は、ホストの IP アドレス（または DNS 名）を指定する必要があります。

ホスト上で **Direct from Client** セッション接続タイプを設定する必要もあります。ホストが任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるようにするためのオプションがあります。後者の場合は、クライアントの MAC アドレスを指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Direct to Host](#) : MC を使用して、クライアントデバイスの **Direct to Host** セッション接続タイプを定義したプロファイルを設定する方法について説明します。MC を使用した特定のホストとクライアントの静的なリンク方法については、『PCoIP Management Console User Manual』（TER0812002）を参照してください。
- [AWI クライアント : Direct to Host](#) : AWI を使用して、クライアントを特定のホストカードに静的に接続するための設定方法について説明します。
- [AWI ホスト : Direct from Client](#) : AWI を使用して、ホストカードを任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるように設定する方法について説明します。

4.11.3 SLP ホストディスカバリを使用したホストとクライアントの接続

ホストがクライアントと同じネットワークサブネット上に存在する場合は、**Direct to Host + SLP** セッション接続タイプを使用して、クライアントがサービスロケーションプロトコル (SLP) を使用してサブネット上のホストを検出するように設定することができます。この設定では、クライアント OSD に、発見された最初の 10 ホストが一覧表示されます。必要なホストを選択してそれに接続することができます。

注意： SLP ホストディスカバリは、ホストが 10 を超える大規模なデプロイメントでクライアントがいずれかのホストに接続しなければならない場合には適していません。この場合は、[サードパーティ製コネクションブローカ](#)が必要です。

ホスト上で **Direct from Client** セッション接続タイプを設定する必要もあります。ホストが任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるようにするためのオプションがあります。後者の場合は、クライアントの MAC アドレスを指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Direct to Host + SLP](#) : MC を使用して、クライアントデバイスの **Direct to Host + SLP** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : Direct to Host + SLP](#) : AWI を使用して、クライアントを SLP ディスカバリ経由でホストカードに接続するための設定方法について説明します。
- [AWI ホスト : Direct from Client](#) : AWI を使用して、ホストカードを任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるように設定する方法について説明します。
- [OSD : Direct to Host + SLP](#) : OSD を使用して、クライアントを SLP ディスカバリ経由でホストカードに接続するための設定方法について説明します。

4.11.4 サードパーティ製コネクションブローカを使用したホストとクライアントの接続

サードパーティ製コネクションブローカは、ゼロクライアントから接続を確立しているユーザの ID に基づいて動的にホスト PC をゼロクライアントに割り当てるリソースマネージャです。コネクションブローカはホストのプールをゼロクライアントのグループに割り当てるためにも使用されます。コネクションブローカの多くは、大規模な PCoIP デプロイメントやホストとクライアントが同じサブネット上に存在しない環境で使用されます。

このオプションの場合は、ホストとクライアントの両方で **Connection Management Interface** セッション接続タイプを使用します。サードパーティ製コネクションブローカの IP アドレス (または DNS 名) を指定する必要があります。

注意： サードパーティ製コネクションブローカの詳細については、[Teradici サポートサイト](#)で知識ベースサポートトピック 15134-24 を参照してください。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Connection Management Interface](#) : MC を使用して、クライアントデバイスとホストデバイスの **Connection Management Interface** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : Connection Management Interface](#) : AWI を使用して、クライアントをサードパーティ製コネクションブローカ経由でクライアントとホスト間の接続を仲介するように設定する方法について説明します。
- [AWI ホスト : Connection Management Interface](#) : AWI を使用して、ホストをサードパーティ製コネクションブローカ経由でクライアントからの接続要求を受け入れるように設定する方法について説明します。
- [OSD : Connection Management Interface](#) : OSD を使用して、クライアントをサードパーティ製コネクションブローカ経由でクライアントとホスト間の接続を仲介するように設定する方法について説明します。

4.11.5 VMware View Connection Server ブローカを使用したホストとクライアントの接続

VMware View Connection Server ブローカを使用してクライアントとホストカード間の接続を仲介することもできます。

注意：これは、ゼロクライアントを VMware View 仮想デスクトップに接続するための設定方法と同じではありません。

このオプションの場合は、VMware View Agent をホストワークステーションにインストールして、クライアントとホストの両方に関するその他のさまざまな設定要件をクリアする必要があります。詳細については、『Using PCoIP Host Cards with VMware View』（TER0911004）を参照してください。

4.11.6 その他の設定リンク

このセッションタイプに関するすべての範囲のファームウェアパラメータを設定するには、以下のトピックを参照してください。

注意：OSD では一部の設定機能が使用できません。

注意：TERA2321 ゼロクライアントには第 1 世代 TERA1100 クライアントと同じディスプレイポロジがあります。このことは、このセクション内のディスプレイポロジページへのリンクに反映されています。

MC を使用している場合	AWI を使用している場合	OSD を使用している場合
	AWI ホスト : 初期セットアップ AWI クライアント : 初期セットアップ	

MC : ネットワーク設定	AWI : ネットワーク設定	OSD : ネットワーク設定
MCを使用したデバイスネーミングの管理方法については、『PCoIP Management Console User Manual』(TER0812002)を参照してください。	AWI : ラベル設定	OSD : ラベル設定
MC : ディスカバリ設定	AWI : ディスカバリ設定	OSD : ディスカバリ設定
MC : SNMP 設定	AWI : SNMP 設定	
MC : Direct to Host MC : Direct to Host + SLP ホストディスカバリ MC : Connection Management Interface	AWI ホスト : Direct from Client AWI クライアント : Direct to Host AWI クライアント : Direct to Host + SLP ホストディスカバリ AWI ホスト : Connection Management Interface AWI クライアント : Connection Management Interface	OSD : Direct to Host OSD : Direct to Host + SLP ホストディスカバリ OSD : Connection Management Interface
MC : 暗号化設定	AWI : 暗号化設定	
MC : 帯域幅設定	AWI : 帯域幅設定	
MC : 言語設定	AWI クライアント : 言語設定	OSD : 言語設定
MC : OSD 設定	AWI : OSD 設定	OSD : OSD 設定
MC : イメージ設定	AWI ホスト : イメージ設定 AWI クライアント : イメージ設定	OSD : イメージ設定
MC : モニタエミュレーション	AWI Tera2 ホスト : モニタエミュレーション	
MC : 時間設定	AWI : 時間設定	
MC : セキュリティ設定	AWI : セキュリティ設定	
MC : オーディオ承認	AWI ホスト : オーディオ承認	

	AWI クライアント：オーディオ承認	
MC：電源承認	AWI クライアント：電源承認	
MC：ホストドライバ機能	AWI ホスト：ホストドライバ機能	
MC：イベントログ設定	AWI：イベントログ設定	OSD：イベントログ設定
MC：周辺機器設定	AWI クライアント：周辺機器設定	
MC：IPv6 設定	AWI：IPv6 設定	OSD：IPv6 設定
MC：ディスプレイトポロジ設定		OSD Tera1：ディスプレイトポロジ設定
MC：OSD ログ設定	AWI クライアント：OSD ログ設定	
MC：ファームウェア管理	AWI：ファームウェアアップロード設定	
MC：USB 承認	AWI ホスト：USB 承認 AWI クライアント：USB 承認	
MC：証明書ストア管理	AWI：証明書アップロード設定	
MC：VMware View 証明書チェック設定	AWI：VMware View 証明書チェック設定	OSD：VMware View 証明書チェック設定

4.12 TERA2140 ゼロクライアントと TERA2220 ホストカードの接続

このトピックでは、第2世代 TERA2140 ゼロクライアントと第2世代 TERA2220 ホストカード間の接続の設定方法について説明します。

注意：使用されているホストカードとゼロクライアントを特定するには、「[プロセッサ情報の表示](#)」を参照してください。クライアントとホストのディスプレイオプションを確認するには、「[PCoIP ホストカードとゼロクライアント](#)」を参照してください。

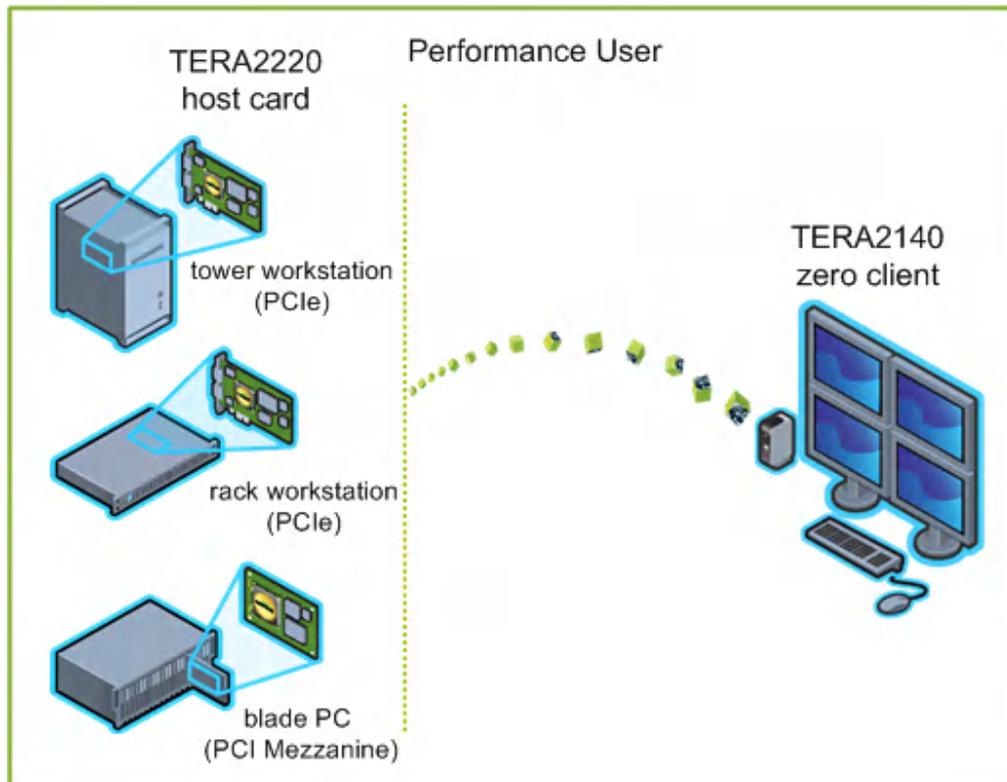


図 4-9 : TERA2140 ゼロクライアントと TERA2220 ホストカードの接続

図の左側は、タワーワークステーション、ラックワークステーション、ブレードワークステーションなどのホストカードをインストール可能なリモートワークステーションに関するフォームファクタを示しています。右側のゼロクライアントは、SLP ディスカバリ、VMware View Connection Server ブローカ、または別のサードパーティ製コネクションブローカを経由する直接ホスト/クライアント割り当てを通してリモートワークステーションに接続することができます。これらの接続オプションについては後述します。

注意：その他のクライアントオプションには、PCoIP 対応ディスプレイ、電話機、ラップトップ、iPad、およびその他の PCoIP 対応モバイルプラットフォームが含まれます。

4.13 前提条件

ホストカードとゼロクライアントを接続する前に、以下の条件を満たす必要があります。

- ホストカードとゼロクライアントのファームウェアバージョンを一致させる必要があります。MC を使用したファームウェアのアップロード方法については、『PCoIP Management Console User Manual』（TER0812002）を参照してください。MC を使用したプロファイルへのファームウェアファイルの割り当て方法については、「[MC：ファームウェア管理](#)」を参照してください。AWI を使用した単一

ホストまたはクライアントへのファームウェアのアップロード方法については、「[AWI: ファームウェアアップロード設定](#)」を参照してください。

- ネットワークリソースは、帯域幅、QoS、遅延、ジッタ、およびパケットロスに関する要件を満たすことができる必要があります。PCoIP ネットワークアーキテクチャの設計方法については、『[PC-over-IP Protocol Virtual Desktop Network Design Checklist](#)』（TER1105004）を参照してください。

4.13.1 セッション接続タイプ

PCoIP デプロイメントの規模によっては、管理コンソールまたはコネクションブローカを使用してホストカードとゼロクライアント間の接続を管理したり、AWI を使用して個々のホストとクライアントを直接セッション接続タイプを使用するように設定したりすることができます。

注意：OSD を使用してセッション接続タイプ構成のクライアント側を設定することもできます。

次の 4 つの接続オプションが使用できます。

- [ホストとクライアントの静的な接続](#)
- [SLP ホストディスカバリを使用したホストとクライアントの接続](#)
- [サードパーティ製コネクションブローカを使用したホストとクライアントの接続](#)
- [VMware View Connection Server ブローカを使用したホストとクライアントの接続](#)

4.13.2 ホストとクライアントの静的な接続

クライアントを特定のホストカードに直接接続するように静的に設定するには、**Direct to Host** セッション接続タイプを使用します。このオプションの場合は、ホストの IP アドレス（または DNS 名）を指定する必要があります。

ホスト上で **Direct from Client** セッション接続タイプを設定する必要もあります。ホストが任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるようにするためのオプションがあります。後者の場合は、クライアントの MAC アドレスを指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Direct to Host](#) : MC を使用して、クライアントデバイスの **Direct to Host** セッション接続タイプを定義したプロファイルを設定する方法について説明します。MC を使用した特定のホストとクライアントの静的なリンク方法については、『[PCoIP Management Console User Manual](#)』（TER0812002）を参照してください。
- [AWI クライアント : Direct to Host](#) : AWI を使用して、クライアントを特定のホストカードに静的に接続するための設定方法について説明します。
- [AWI ホスト : Direct from Client](#) : AWI を使用して、ホストカードを任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるように設定する方法について説明します。

4.13.3 SLP ホストディスカバリを使用したホストとクライアントの接続

ホストがクライアントと同じネットワークサブネット上に存在する場合は、**Direct to Host + SLP** セッション接続タイプを使用して、クライアントがサービスロケーションプロトコル (SLP) を使用してサブネット上のホストを検出するように設定することができます。この設定では、クライアント OSD に、発見された最初の 10 ホストが一覧表示されます。必要なホストを選択してそれに接続することができます。

注意： SLP ホストディスカバリは、ホストが 10 を超える大規模なデプロイメントでクライアントがいずれかのホストに接続しなければならない場合には適していません。この場合は、[サードパーティ製コネクションブローカ](#)が必要です。

ホスト上で **Direct from Client** セッション接続タイプを設定する必要もあります。ホストが任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるようにするためのオプションがあります。後者の場合は、クライアントの MAC アドレスを指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Direct to Host + SLP](#) : MC を使用して、クライアントデバイスの **Direct to Host + SLP** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : Direct to Host + SLP](#) : AWI を使用して、クライアントを SLP ディスカバリ経由でホストカードに接続するための設定方法について説明します。
- [AWI ホスト : Direct from Client](#) : AWI を使用して、ホストカードを任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるように設定する方法について説明します。
- [OSD : Direct to Host + SLP](#) : OSD を使用して、クライアントを SLP ディスカバリ経由でホストカードに接続するための設定方法について説明します。

4.13.4 サードパーティ製コネクションブローカを使用したホストとクライアントの接続

サードパーティ製コネクションブローカは、ゼロクライアントから接続を確立しているユーザの ID に基づいて動的にホスト PC をゼロクライアントに割り当てるリソースマネージャです。コネクションブローカはホストのプールをゼロクライアントのグループに割り当てるためにも使用されます。コネクションブローカの多くは、大規模な PCoIP デプロイメントやホストとクライアントが同じサブネット上に存在しない環境で使用されます。

このオプションの場合は、ホストとクライアントの両方で **Connection Management Interface** セッション接続タイプを使用します。サードパーティ製コネクションブローカの IP アドレス (または DNS 名) を指定する必要があります。

注意： サードパーティ製コネクションブローカの詳細については、[Teradici サポートサイト](#)で知識ベースサポートトピック 15134-24 を参照してください。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Connection Management Interface](#) : MC を使用して、クライアントデバイスとホストデバイスの **Connection Management Interface** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : Connection Management Interface](#) : AWI を使用して、クライアントをサードパーティ製コネクションブローカ経由でクライアントとホスト間の接続を仲介するように設定する方法について説明します。
- [AWI ホスト : Connection Management Interface](#) : AWI を使用して、ホストをサードパーティ製コネクションブローカ経由でクライアントからの接続要求を受け入れるように設定する方法について説明します。
- [OSD : Connection Management Interface](#) : OSD を使用して、クライアントをサードパーティ製コネクションブローカ経由でクライアントとホスト間の接続を仲介するように設定する方法について説明します。

4.13.5 VMware View Connection Server ブローカを使用したホストとクライアントの接続

VMware View Connection Server ブローカを使用してクライアントとホストカード間の接続を仲介することもできます。

注意 : これは、ゼロクライアントを VMware View 仮想デスクトップに接続するための設定方法と同じではありません。

このオプションの場合は、VMware View Agent をホストワークステーションにインストールして、クライアントとホストの両方に関するその他のさまざまな設定要件をクリアする必要があります。詳細については、『Using PCoIP Host Cards with VMware View』（TER0911004）を参照してください。

4.13.6 その他の設定リンク

このセッションタイプに関するすべての範囲のファームウェアパラメータを設定するには、以下のトピックを参照してください。

注意 : OSD では一部の設定機能が使用できません。

MC を使用している場合	AWI を使用している場合	OSD を使用している場合
	AWI ホスト : 初期セットアップ AWI クライアント : 初期セットアップ	
MC : ネットワーク設定	AWI : ネットワーク設定	OSD : ネットワーク設定
MC を使用したデバイスネーミ	AWI : ラベル設定	OSD : ラベル設定

<p>ングの管理方法については、 『PCoIP Management Console User Manual』 (TER0812002) を参照してく ださい。</p>		
<p>MC : ディスカバリ設定</p>	<p>AWI : ディスカバリ設定</p>	<p>OSD : ディスカバリ設定</p>
<p>MC : SNMP 設定</p>	<p>AWI : SNMP 設定</p>	
<p>MC : Direct to Host MC : Direct to Host + SLP ホス トディスカバリ MC : Connection Management Interface</p>	<p>AWI ホスト : Direct from Client AWI クライアント : Direct to Host AWI クライアント : Direct to Host + SLP ホストディスカバ リ AWI ホスト : Connection Management Interface AWI クライアント : Connection Management Interface</p>	<p>OSD : Direct to Host OSD : Direct to Host + SLP ホ ストディスカバリ OSD : Connection Management Interface</p>
<p>MC : 暗号化設定</p>	<p>AWI : 暗号化設定</p>	
<p>MC : 帯域幅設定</p>	<p>AWI : 帯域幅設定</p>	
<p>MC : 言語設定</p>	<p>AWI クライアント : 言語設定</p>	<p>OSD : 言語設定</p>
<p>MC : OSD 設定</p>	<p>AWI : OSD 設定</p>	<p>OSD : OSD 設定</p>
<p>MC : イメージ設定</p>	<p>AWI ホスト : イメージ設定 AWI クライアント : イメージ設 定</p>	<p>OSD : イメージ設定</p>
<p>MC : モニタエミュレーション</p>	<p>AWI Tera2 ホスト : モニタエミ ュレーション</p>	
<p>MC : 時間設定</p>	<p>AWI : 時間設定</p>	
<p>MC : セキュリティ設定</p>	<p>AWI : セキュリティ設定</p>	
<p>MC : オーディオ承認</p>	<p>AWI ホスト : オーディオ承認 AWI クライアント : オーディオ 承認</p>	

MC : 電源承認	AWI クライアント : 電源承認	
MC : ホストドライバ機能	AWI ホスト : ホストドライバ機能	
MC : イベントログ設定	AWI : イベントログ設定	OSD : イベントログ設定
MC : 周辺機器設定	AWI クライアント : 周辺機器設定	
MC : IPv6 設定	AWI : IPv6 設定	OSD : IPv6 設定
MC : ディスプレイトポロジ設定		OSD Tera2 : ディスプレイトポロジ設定
MC : OSD ログ設定	AWI クライアント : OSD ログ設定	
MC : フォームウェア管理	AWI : フォームウェアアップロード設定	
MC : USB 承認	AWI ホスト : USB 承認 AWI クライアント : USB 承認	
MC : 証明書ストア管理	AWI : 証明書アップロード設定	
MC : VMware View 証明書チェック設定	AWI : VMware View 証明書チェック設定	OSD : VMware View 証明書チェック設定

4.14 TERA1100 ゼロクライアントと TERA2240 ホストカードの接続

このトピックでは、第1世代 TERA1100 ゼロクライアントと第2世代 TERA2240 ホストカード間の接続の設定方法について説明します。

注意：使用されているホストカードとゼロクライアントを特定するには、「[プロセス情報の表示](#)」を参照してください。クライアントとホストのディスプレイオプションを確認するには、「[PCoIP ホストカードとゼロクライアント](#)」を参照してください。

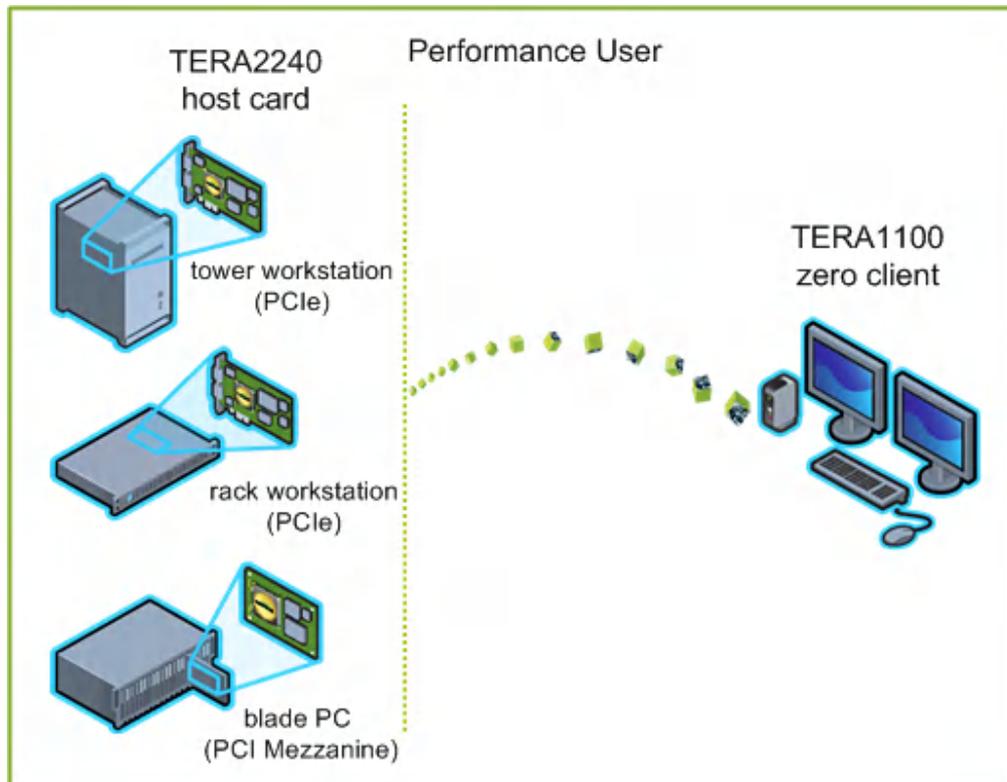


図 4-10 : TERA1100 ゼロクライアントと TERA2240 ホストカードの接続

図の左側は、タワーワークステーション、ラックワークステーション、ブレードワークステーションなどのホストカードをインストール可能なリモートワークステーションに関するフォームファクタを示しています。右側のゼロクライアントは、SLP ディスカバリ、VMware View Connection Server ブローカ、または別のサードパーティ製接続ブローカを経由する直接ホスト/クライアント割り当てを通してリモートワークステーションに接続することができます。これらの接続オプションについては後述します。

注意：その他のクライアントオプションには、PCoIP 対応ディスプレイ、電話機、ラップトップ、iPad、およびその他の PCoIP 対応モバイルプラットフォームが含まれます。

4.15 前提条件

ホストカードとゼロクライアントを接続する前に、以下の条件を満たす必要があります。

- ホストカードとゼロクライアントのファームウェアバージョンを一致させる必要があります。MC を使用したファームウェアのアップロード方法については、『PCoIP Management Console User Manual』（TER0812002）を参照してください。MC を使用したプロファイルへのファームウェアファイルの割り当て方法については、「[MC：ファームウェア管理](#)」を参照してください。AWI を使用した単一

ホストまたはクライアントへのファームウェアのアップロード方法については、
「[AWI: ファームウェアアップロード設定](#)」を参照してください。

- ネットワークリソースは、帯域幅、QoS、遅延、ジッタ、およびパケットロスに関する要件を満たすことができる必要があります。PCoIP ネットワークアーキテクチャの設計方法については、『PC-over-IP Protocol Virtual Desktop Network Design Checklist』（TER1105004）を参照してください。

4.15.1 セッション接続タイプ

PCoIP デプロイメントの規模によっては、管理コンソールまたは接続ブローカを使用してホストカードとゼロクライアント間の接続を管理したり、AWI を使用して個々のホストとクライアントを、直接セッション接続タイプを使用するように設定したりすることができます。

注意：OSD を使用してセッション接続タイプ構成のクライアント側を設定することもできます。

次の 4 つの接続オプションが使用できます。

- [ホストとクライアントの静的な接続](#)
- [SLP ホストディスカバリを使用したホストとクライアントの接続](#)
- [サードパーティ製接続ブローカを使用したホストとクライアントの接続](#)
- [VMware View Connection Server ブローカを使用したホストとクライアントの接続](#)

4.15.2 ホストとクライアントの静的な接続

クライアントを特定のホストカードに直接接続するように静的に設定するには、**Direct to Host** セッション接続タイプを使用します。このオプションの場合は、ホストの IP アドレス（または DNS 名）を指定する必要があります。

ホスト上で **Direct from Client** セッション接続タイプを設定する必要もあります。ホストが任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるようにするためのオプションがあります。後者の場合は、クライアントの MAC アドレスを指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Direct to Host](#) : MC を使用して、クライアントデバイスの **Direct to Host** セッション接続タイプを定義したプロファイルを設定する方法について説明します。MC を使用した特定のホストとクライアントの静的なリンク方法については、『PCoIP Management Console User Manual』（TER0812002）を参照してください。
- [AWI クライアント : Direct to Host](#) : AWI を使用して、クライアントを特定のホストカードに静的に接続するための設定方法について説明します。
- [AWI ホスト : Direct from Client](#) : AWI を使用して、ホストカードを任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるように設定する方法について説明します。

4.15.3 SLP ホストディスカバリを使用したホストとクライアントの接続

ホストがクライアントと同じネットワークサブネット上に存在する場合は、**Direct to Host + SLP** セッション接続タイプを使用して、クライアントがサービスロケーションプロトコル (SLP) を使用してサブネット上のホストを検出するように設定することができます。この設定では、クライアント OSD に、発見された最初の 10 ホストが一覧表示されます。必要なホストを選択してそれに接続することができます。

注意： SLP ホストディスカバリは、ホストが 10 を超える大規模なデプロイメントでクライアントがいずれかのホストに接続しなければならない場合には適していません。この場合は、[サードパーティ製コネクションブローカ](#)が必要です。

ホスト上で **Direct from Client** セッション接続タイプを設定する必要もあります。ホストが任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるようにするためのオプションがあります。後者の場合は、クライアントの MAC アドレスを指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Direct to Host + SLP](#) : MC を使用して、クライアントデバイスの **Direct to Host + SLP** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : Direct to Host + SLP](#) : AWI を使用して、クライアントを SLP ディスカバリ経由でホストカードに接続するための設定方法について説明します。
- [AWI ホスト : Direct from Client](#) : AWI を使用して、ホストカードを任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるように設定する方法について説明します。
- [OSD : Direct to Host + SLP](#) : OSD を使用して、クライアントを SLP ディスカバリ経由でホストカードに接続するための設定方法について説明します。

4.15.4 サードパーティ製コネクションブローカを使用したホストとクライアントの接続

サードパーティ製コネクションブローカは、ゼロクライアントから接続を確立しているユーザの ID に基づいて動的にホスト PC をゼロクライアントに割り当てるリソースマネージャです。コネクションブローカはホストのプールをゼロクライアントのグループに割り当てるためにも使用されます。コネクションブローカの多くは、大規模な PCoIP デプロイメントやホストとクライアントが同じサブネット上に存在しない環境で使用されます。

このオプションの場合は、ホストとクライアントの両方で **Connection Management Interface** セッション接続タイプを使用します。サードパーティ製コネクションブローカの IP アドレス (または DNS 名) を指定する必要があります。

注意： サードパーティ製コネクションブローカの詳細については、[Teradici サポートサイト](#)で知識ベースサポートトピック 15134-24 を参照してください。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Connection Management Interface](#) : MC を使用して、クライアントデバイスとホストデバイスの **Connection Management Interface** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : Connection Management Interface](#) : AWI を使用して、クライアントをサードパーティ製コネクションブローカ経由でクライアントとホスト間の接続を仲介するように設定する方法について説明します。
- [AWI ホスト : Connection Management Interface](#) : AWI を使用して、ホストをサードパーティ製コネクションブローカ経由でクライアントからの接続要求を受け入れるように設定する方法について説明します。
- [OSD : Connection Management Interface](#) : OSD を使用して、クライアントをサードパーティ製コネクションブローカ経由でクライアントとホスト間の接続を仲介するように設定する方法について説明します。

4.15.5 VMware View Connection Server ブローカを使用したホストとクライアントの接続

VMware View Connection Server ブローカを使用してクライアントとホストカード間の接続を仲介することもできます。

注意 : これは、ゼロクライアントを VMware View 仮想デスクトップに接続するための設定方法と同じではありません。

このオプションの場合は、VMware View Agent をホストワークステーションにインストールして、クライアントとホストの両方に関するその他のさまざまな設定要件をクリアする必要があります。詳細については、『Using PCoIP Host Cards with VMware View』（TER0911004）を参照してください。

4.15.6 その他の設定リンク

このセッションタイプに関するすべての範囲のファームウェアパラメータを設定するには、以下のトピックを参照してください。

注意 : OSD では一部の設定機能が使用できません。

MC を使用している場合	AWI を使用している場合	OSD を使用している場合
	AWI ホスト : 初期セットアップ AWI クライアント : 初期セットアップ	
MC : ネットワーク設定	AWI : ネットワーク設定	OSD : ネットワーク設定
MC を使用したデバイスネーミ	AWI : ラベル設定	OSD : ラベル設定

<p>ングの管理方法については、 『PCoIP Management Console User Manual』 (TER0812002) を参照してく ださい。</p>		
<p>MC : ディスカバリ設定</p>	<p>AWI : ディスカバリ設定</p>	<p>OSD : ディスカバリ設定</p>
<p>MC : SNMP 設定</p>	<p>AWI : SNMP 設定</p>	
<p>MC : Direct to Host MC : Direct to Host + SLP ホス トディスカバリ MC : Connection Management Interface</p>	<p>AWI ホスト : Direct from Client AWI クライアント : Direct to Host AWI クライアント : Direct to Host + SLP ホストディスカバ リ AWI ホスト : Connection Management Interface AWI クライアント : Connection Management Interface</p>	<p>OSD : Direct to Host OSD : Direct to Host + SLP ホ ストディスカバリ OSD : Connection Management Interface</p>
<p>MC : 暗号化設定</p>	<p>AWI : 暗号化設定</p>	
<p>MC : 帯域幅設定</p>	<p>AWI : 帯域幅設定</p>	
<p>MC : 言語設定</p>	<p>AWI クライアント : 言語設定</p>	<p>OSD : 言語設定</p>
<p>MC : OSD 設定</p>	<p>AWI : OSD 設定</p>	<p>OSD : OSD 設定</p>
<p>MC : イメージ設定</p>	<p>AWI ホスト : イメージ設定 AWI クライアント : イメージ設 定</p>	<p>OSD : イメージ設定</p>
<p>MC : モニタエミュレーション</p>	<p>AWI Tera2 ホスト : モニタエミ ュレーション</p>	
<p>MC : 時間設定</p>	<p>AWI : 時間設定</p>	
<p>MC : セキュリティ設定</p>	<p>AWI : セキュリティ設定</p>	
<p>MC : オーディオ承認</p>	<p>AWI ホスト : オーディオ承認 AWI クライアント : オーディオ 承認</p>	

MC : 電源承認	AWI クライアント : 電源承認	
MC : ホストドライバ機能	AWI ホスト : ホストドライバ機能	
MC : イベントログ設定	AWI : イベントログ設定	OSD : イベントログ設定
MC : 周辺機器設定	AWI クライアント : 周辺機器設定	
MC : IPv6 設定	AWI : IPv6 設定	OSD : IPv6 設定
MC : ディスプレイトポロジ設定		OSD Tera1 : ディスプレイトポロジ設定
MC : OSD ログ設定	AWI クライアント : OSD ログ設定	
MC : フォームウェア管理	AWI : フォームウェアアップロード設定	
MC : USB 承認	AWI ホスト : USB 承認 AWI クライアント : USB 承認	
MC : 証明書ストア管理	AWI : 証明書アップロード設定	
MC : VMware View 証明書チェック設定	AWI : VMware View 証明書チェック設定	OSD : VMware View 証明書チェック設定

4.16 TERA2321 ゼロクライアントと TERA2240 ホストカードの接続

このトピックでは、第2世代 TERA2321 ゼロクライアントと第2世代 TERA2240 ホストカード間の接続の設定方法について説明します。

注意：使用されているホストカードとゼロクライアントを特定するには、「[プロセス情報の表示](#)」を参照してください。クライアントとホストのディスプレイオプションを確認するには、「[PCoIP ホストカードとゼロクライアント](#)」を参照してください。

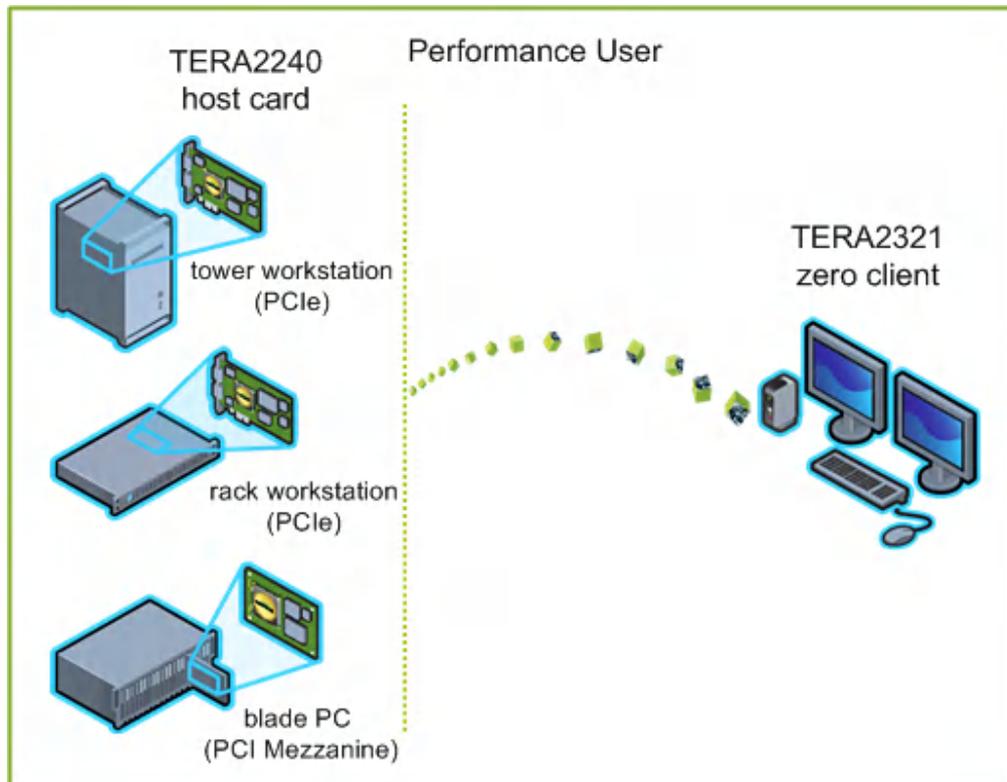


図 4-11 : TERA2321 ゼロクライアントと TERA2240 ホストカードの接続

図の左側は、タワーワークステーション、ラックワークステーション、ブレードワークステーションなどのホストカードをインストール可能なリモートワークステーションに関するフォームファクタを示しています。右側のゼロクライアントは、SLP ディスカバリ、VMware View Connection Server ブローカ、または別のサードパーティ製コネクショントラフィックブローカを経由する直接ホスト/クライアント割り当てを通してリモートワークステーションに接続することができます。これらの接続オプションについては後述します。

注意：その他のクライアントオプションには、PCoIP 対応ディスプレイ、電話機、ラップトップ、iPad、およびその他の PCoIP 対応モバイルプラットフォームが含まれます。

4.17 前提条件

ホストカードとゼロクライアントを接続する前に、以下の条件を満たす必要があります。

- ホストカードとゼロクライアントのファームウェアバージョンを一致させる必要があります。MC を使用したファームウェアのアップロード方法については、『PCoIP Management Console User Manual』（TER0812002）を参照してください。MC を使用したプロファイルへのファームウェアファイルの割り当て方法については、「[MC：ファームウェア管理](#)」を参照してください。AWI を使用した単一

ホストまたはクライアントへのファームウェアのアップロード方法については、「[AWI: ファームウェアアップロード設定](#)」を参照してください。

- ネットワークリソースは、帯域幅、QoS、遅延、ジッタ、およびパケットロスに関する要件を満たすことができる必要があります。PCoIP ネットワークアーキテクチャの設計方法については、『[PC-over-IP Protocol Virtual Desktop Network Design Checklist](#)』（TER1105004）を参照してください。

4.17.1 セッション接続タイプ

PCoIP デプロイメントの規模によっては、管理コンソールまたはコネクションブローカを使用してホストカードとゼロクライアント間の接続を管理したり、AWI を使用して個々のホストとクライアントを、直接セッション接続タイプを使用するように設定したりすることができます。

注意：OSD を使用してセッション接続タイプ構成のクライアント側を設定することもできます。

次の 4 つの接続オプションが使用できます。

- [ホストとクライアントの静的な接続](#)
- [SLP ホストディスカバリを使用したホストとクライアントの接続](#)
- [サードパーティ製コネクションブローカを使用したホストとクライアントの接続](#)
- [VMware View Connection Server ブローカを使用したホストとクライアントの接続](#)

4.17.2 ホストとクライアントの静的な接続

クライアントを特定のホストカードに直接接続するように静的に設定するには、**Direct to Host** セッション接続タイプを使用します。このオプションの場合は、ホストの IP アドレス（または DNS 名）を指定する必要があります。

ホスト上で **Direct from Client** セッション接続タイプを設定する必要もあります。ホストが任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるようにするためのオプションがあります。後者の場合は、クライアントの MAC アドレスを指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Direct to Host](#) : MC を使用して、クライアントデバイスの **Direct to Host** セッション接続タイプを定義したプロファイルを設定する方法について説明します。MC を使用した特定のホストとクライアントの静的なリンク方法については、『[PCoIP Management Console User Manual](#)』（TER0812002）を参照してください。
- [AWI クライアント : Direct to Host](#) : AWI を使用して、クライアントを特定のホストカードに静的に接続するための設定方法について説明します。
- [AWI ホスト : Direct from Client](#) : AWI を使用して、ホストカードを任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるように設定する方法について説明します。

4.17.3 SLP ホストディスカバリを使用したホストとクライアントの接続

ホストがクライアントと同じネットワークサブネット上に存在する場合は、**Direct to Host + SLP** セッション接続タイプを使用して、クライアントがサービスロケーションプロトコル (SLP) を使用してサブネット上のホストを検出するように設定することができます。この設定では、クライアント OSD に、発見された最初の 10 ホストが一覧表示されます。必要なホストを選択してそれに接続することができます。

注意： SLP ホストディスカバリは、ホストが 10 を超える大規模なデプロイメントでクライアントがいずれかのホストに接続しなければならない場合には適していません。この場合は、[サードパーティ製コネクションブローカ](#)が必要です。

ホスト上で **Direct from Client** セッション接続タイプを設定する必要もあります。ホストが任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるようにするためのオプションがあります。後者の場合は、クライアントの MAC アドレスを指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Direct to Host + SLP](#) : MC を使用して、クライアントデバイスの **Direct to Host + SLP** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : Direct to Host + SLP](#) : AWI を使用して、クライアントを SLP ディスカバリ経由でホストカードに接続するための設定方法について説明します。
- [AWI ホスト : Direct from Client](#) : AWI を使用して、ホストカードを任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるように設定する方法について説明します。
- [OSD : Direct to Host + SLP](#) : OSD を使用して、クライアントを SLP ディスカバリ経由でホストカードに接続するための設定方法について説明します。

4.17.4 サードパーティ製コネクションブローカを使用したホストとクライアントの接続

サードパーティ製コネクションブローカは、ゼロクライアントから接続を確立しているユーザの ID に基づいて動的にホスト PC をゼロクライアントに割り当てるリソースマネージャです。コネクションブローカはホストのプールをゼロクライアントのグループに割り当てるためにも使用されます。コネクションブローカの多くは、大規模な PCoIP デプロイメントやホストとクライアントが同じサブネット上に存在しない環境で使用されます。

このオプションの場合は、ホストとクライアントの両方で **Connection Management Interface** セッション接続タイプを使用します。サードパーティ製コネクションブローカの IP アドレス (または DNS 名) を指定する必要があります。

注意： サードパーティ製コネクションブローカの詳細については、[Teradici サポートサイト](#)で知識ベースサポートトピック 15134-24 を参照してください。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Connection Management Interface](#) : MC を使用して、クライアントデバイスとホストデバイスの **Connection Management Interface** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : Connection Management Interface](#) : AWI を使用して、クライアントをサードパーティ製コネクションブローカ経由でクライアントとホスト間の接続を仲介するように設定する方法について説明します。
- [AWI ホスト : Connection Management Interface](#) : AWI を使用して、ホストをサードパーティ製コネクションブローカ経由でクライアントからの接続要求を受け入れるように設定する方法について説明します。
- [OSD : Connection Management Interface](#) : OSD を使用して、クライアントをサードパーティ製コネクションブローカ経由でクライアントとホスト間の接続を仲介するように設定する方法について説明します。

4.17.5 VMware View Connection Server ブローカを使用したホストとクライアントの接続

VMware View Connection Server ブローカを使用してクライアントとホストカード間の接続を仲介することもできます。

注意：これは、ゼロクライアントを VMware View 仮想デスクトップに接続するための設定方法と同じではありません。

このオプションの場合は、VMware View Agent をホストワークステーションにインストールして、クライアントとホストの両方に関するその他のさまざまな設定要件をクリアする必要があります。詳細については、『Using PCoIP Host Cards with VMware View』（TER0911004）を参照してください。

4.17.6 その他の設定リンク

このセッションタイプに関するすべての範囲のファームウェアパラメータを設定するには、以下のトピックを参照してください。

注意：OSD では一部の設定機能が使用できません。

注意：TERA2321 ゼロクライアントには第 1 世代 TERA1100 クライアントと同じディスプレイポロジがあります。このことは、このセクション内のディスプレイポロジページへのリンクに反映されています。

MC を使用している場合	AWI を使用している場合	OSD を使用している場合
	AWI ホスト : 初期セットアップ AWI クライアント : 初期セットアップ	

MC : ネットワーク設定	AWI : ネットワーク設定	OSD : ネットワーク設定
MCを使用したデバイスネーミングの管理方法については、『PCoIP Management Console User Manual』(TER0812002)を参照してください。	AWI : ラベル設定	OSD : ラベル設定
MC : ディスカバリ設定	AWI : ディスカバリ設定	OSD : ディスカバリ設定
MC : SNMP 設定	AWI : SNMP 設定	
MC : Direct to Host MC : Direct to Host + SLP ホストディスカバリ MC : Connection Management Interface	AWI ホスト : Direct from Client AWI クライアント : Direct to Host AWI クライアント : Direct to Host + SLP ホストディスカバリ AWI ホスト : Connection Management Interface AWI クライアント : Connection Management Interface	OSD : Direct to Host OSD : Direct to Host + SLP ホストディスカバリ OSD : Connection Management Interface
MC : 暗号化設定	AWI : 暗号化設定	
MC : 帯域幅設定	AWI : 帯域幅設定	
MC : 言語設定	AWI クライアント : 言語設定	OSD : 言語設定
MC : OSD 設定	AWI : OSD 設定	OSD : OSD 設定
MC : イメージ設定	AWI ホスト : イメージ設定 AWI クライアント : イメージ設定	OSD : イメージ設定
MC : モニタエミュレーション	AWI Tera2 ホスト : モニタエミュレーション	
MC : 時間設定	AWI : 時間設定	
MC : セキュリティ設定	AWI : セキュリティ設定	
MC : オーディオ承認	AWI ホスト : オーディオ承認	

	AWI クライアント : オーディオ承認	
MC : 電源承認	AWI クライアント : 電源承認	
MC : ホストドライバ機能	AWI ホスト : ホストドライバ機能	
MC : イベントログ設定	AWI : イベントログ設定	OSD : イベントログ設定
MC : 周辺機器設定	AWI クライアント : 周辺機器設定	
MC : IPv6 設定	AWI : IPv6 設定	OSD : IPv6 設定
MC : ディスプレイトポロジ設定		OSD Tera1 : ディスプレイトポロジ設定
MC : OSD ログ設定	AWI クライアント : OSD ログ設定	
MC : フォームウェア管理	AWI : ファームウェアアップロード設定	
MC : USB 承認	AWI ホスト : USB 承認 AWI クライアント : USB 承認	
MC : 証明書ストア管理	AWI : 証明書アップロード設定	
MC : VMware View 証明書チェック設定	AWI : VMware View 証明書チェック設定	OSD : VMware View 証明書チェック設定

4.18 TERA2140 ゼロクライアントと TERA2240 ホストカードの接続

このトピックでは、第2世代 TERA2140 ゼロクライアントと第2世代 TERA2240 ホストカード間の接続の設定方法について説明します。

注意：使用されているホストカードとゼロクライアントを特定するには、「[プロセッサ情報の表示](#)」を参照してください。クライアントとホストのディスプレイオプションを確認するには、「[PCoIP ホストカードとゼロクライアント](#)」を参照してください。

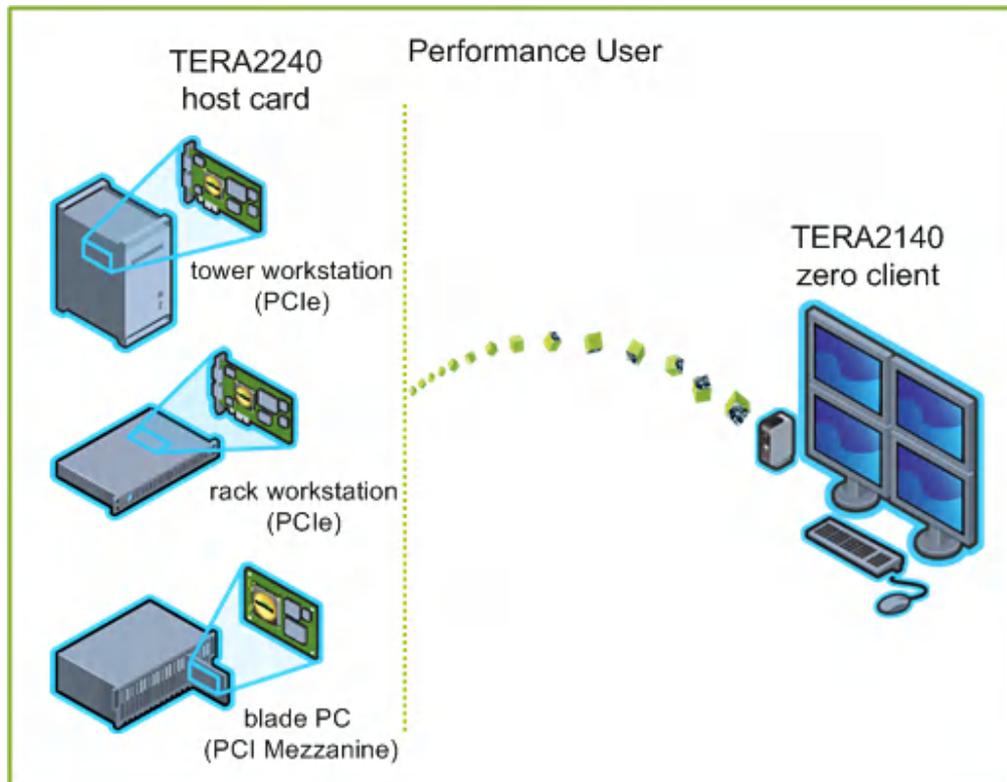


図 4-12 : TERA2140 ゼロクライアントと TERA2240 ホストカードの接続

図の左側は、タワーワークステーション、ラックワークステーション、ブレードワークステーションなどのホストカードをインストール可能なリモートワークステーションに関するフォームファクタを示しています。右側のゼロクライアントは、SLP ディスカバリ、VMware View Connection Server ブローカ、または別のサードパーティ製接続ブローカを経由する直接ホスト/クライアント割り当てを通してリモートワークステーションに接続することができます。これらの接続オプションについては後述します。

注意：その他のクライアントオプションには、PCoIP 対応ディスプレイ、電話機、ラップトップ、iPad、およびその他の PCoIP 対応モバイルプラットフォームが含まれます。

4.19 前提条件

ホストカードとゼロクライアントを接続する前に、以下の条件を満たす必要があります。

- ホストカードとゼロクライアントのファームウェアバージョンを一致させる必要があります。MC を使用したファームウェアのアップロード方法については、『PCoIP Management Console User Manual』（TER0812002）を参照してください。MC を使用したプロファイルへのファームウェアファイルの割り当て方法については、「[MC：ファームウェア管理](#)」を参照してください。AWI を使用した単一

ホストまたはクライアントへのファームウェアのアップロード方法については、「[AWI: ファームウェアアップロード設定](#)」を参照してください。

- ネットワークリソースは、帯域幅、QoS、遅延、ジッタ、およびパケットロスに関する要件を満たすことができる必要があります。PCoIP ネットワークアーキテクチャの設計方法については、『[PC-over-IP Protocol Virtual Desktop Network Design Checklist](#)』（TER1105004）を参照してください。

4.19.1 セッション接続タイプ

PCoIP デプロイメントの規模によっては、管理コンソールまたはコネクションブローカを使用してホストカードとゼロクライアント間の接続を管理したり、AWI を使用して個々のホストとクライアントを直接セッション接続タイプを使用するように設定したりすることができます。

注意：OSD を使用してセッション接続タイプ構成のクライアント側を設定することもできます。

次の 4 つの接続オプションが使用できます。

- [ホストとクライアントの静的な接続](#)
- [SLP ホストディスカバリを使用したホストとクライアントの接続](#)
- [サードパーティ製コネクションブローカを使用したホストとクライアントの接続](#)
- [VMware View Connection Server ブローカを使用したホストとクライアントの接続](#)

4.19.2 ホストとクライアントの静的な接続

クライアントを特定のホストカードに直接接続するように静的に設定するには、**Direct to Host** セッション接続タイプを使用します。このオプションの場合は、ホストの IP アドレス（または DNS 名）を指定する必要があります。

ホスト上で **Direct from Client** セッション接続タイプを設定する必要もあります。ホストが任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるようにするためのオプションがあります。後者の場合は、クライアントの MAC アドレスを指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Direct to Host](#) : MC を使用して、クライアントデバイスの **Direct to Host** セッション接続タイプを定義したプロファイルを設定する方法について説明します。MC を使用した特定のホストとクライアントの静的なリンク方法については、『[PCoIP Management Console User Manual](#)』（TER0812002）を参照してください。
- [AWI クライアント : Direct to Host](#) : AWI を使用して、クライアントを特定のホストカードに静的に接続するための設定方法について説明します。
- [AWI ホスト : Direct from Client](#) : AWI を使用して、ホストカードを任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるように設定する方法について説明します。

4.19.3 SLP ホストディスカバリを使用したホストとクライアントの接続

ホストがクライアントと同じネットワークサブネット上に存在する場合は、**Direct to Host + SLP** セッション接続タイプを使用して、クライアントがサービスロケーションプロトコル (SLP) を使用してサブネット上のホストを検出するように設定することができます。この設定では、クライアント OSD に、発見された最初の 10 ホストが一覧表示されます。必要なホストを選択してそれに接続することができます。

注意： SLP ホストディスカバリは、ホストが 10 を超える大規模なデプロイメントでクライアントがいずれかのホストに接続しなければならない場合には適していません。この場合は、[サードパーティ製コネクションブローカ](#)が必要です。

ホスト上で **Direct from Client** セッション接続タイプを設定する必要もあります。ホストが任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるようにするためのオプションがあります。後者の場合は、クライアントの MAC アドレスを指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Direct to Host + SLP](#) : MC を使用して、クライアントデバイスの **Direct to Host + SLP** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : Direct to Host + SLP](#) : AWI を使用して、クライアントを SLP ディスカバリ経由でホストカードに接続するための設定方法について説明します。
- [AWI ホスト : Direct from Client](#) : AWI を使用して、ホストカードを任意のクライアントからの接続要求または特定のクライアントだけからの接続要求を受け入れるように設定する方法について説明します。
- [OSD : Direct to Host + SLP](#) : OSD を使用して、クライアントを SLP ディスカバリ経由でホストカードに接続するための設定方法について説明します。

4.19.4 サードパーティ製コネクションブローカを使用したホストとクライアントの接続

サードパーティ製コネクションブローカは、ゼロクライアントから接続を確立しているユーザの ID に基づいて動的にホスト PC をゼロクライアントに割り当てるリソースマネージャです。コネクションブローカはホストのプールをゼロクライアントのグループに割り当てるためにも使用されます。コネクションブローカの多くは、大規模な PCoIP デプロイメントやホストとクライアントが同じサブネット上に存在しない環境で使用されます。

このオプションの場合は、ホストとクライアントの両方で **Connection Management Interface** セッション接続タイプを使用します。サードパーティ製コネクションブローカの IP アドレス (または DNS 名) を指定する必要があります。

注意： サードパーティ製コネクションブローカの詳細については、[Teradici サポートサイト](#)で知識ベースサポートトピック 15134-24 を参照してください。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : Connection Management Interface](#) : MC を使用して、クライアントデバイスとホストデバイスの **Connection Management Interface** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : Connection Management Interface](#) : AWI を使用して、クライアントをサードパーティ製コネクションブローカ経由でクライアントとホスト間の接続を仲介するように設定する方法について説明します。
- [AWI ホスト : Connection Management Interface](#) : AWI を使用して、ホストをサードパーティ製コネクションブローカ経由でクライアントからの接続要求を受け入れるように設定する方法について説明します。
- [OSD : Connection Management Interface](#) : OSD を使用して、クライアントをサードパーティ製コネクションブローカ経由でクライアントとホスト間の接続を仲介するように設定する方法について説明します。

4.19.5 VMware View Connection Server ブローカを使用したホストとクライアントの接続

VMware View Connection Server ブローカを使用してクライアントとホストカード間の接続を仲介することもできます。

注意 : これは、ゼロクライアントを VMware View 仮想デスクトップに接続するための設定方法と同じではありません。

このオプションの場合は、VMware View Agent をホストワークステーションにインストールして、クライアントとホストの両方に関するその他のさまざまな設定要件をクリアする必要があります。詳細については、『Using PCoIP Host Cards with VMware View』（TER0911004）を参照してください。

4.19.6 その他の設定リンク

このセッションタイプに関するすべての範囲のファームウェアパラメータを設定するには、以下のトピックを参照してください。

注意 : OSD では一部の設定機能が使用できません。

MC を使用している場合	AWI を使用している場合	OSD を使用している場合
	AWI ホスト : 初期セットアップ AWI クライアント : 初期セットアップ	
MC : ネットワーク設定	AWI : ネットワーク設定	OSD : ネットワーク設定
MC を使用したデバイスネーミ	AWI : ラベル設定	OSD : ラベル設定

<p>ングの管理方法については、 『PCoIP Management Console User Manual』 (TER0812002) を参照してく ださい。</p>		
<p>MC : ディスカバリ設定</p>	<p>AWI : ディスカバリ設定</p>	<p>OSD : ディスカバリ設定</p>
<p>MC : SNMP 設定</p>	<p>AWI : SNMP 設定</p>	
<p>MC : Direct to Host MC : Direct to Host + SLP ホス トディスカバリ MC : Connection Management Interface</p>	<p>AWI ホスト : Direct from Client AWI クライアント : Direct to Host AWI クライアント : Direct to Host + SLP ホストディスカバ リ AWI ホスト : Connection Management Interface AWI クライアント : Connection Management Interface</p>	<p>OSD : Direct to Host OSD : Direct to Host + SLP ホ ストディスカバリ OSD : Connection Management Interface</p>
<p>MC : 暗号化設定</p>	<p>AWI : 暗号化設定</p>	
<p>MC : 帯域幅設定</p>	<p>AWI : 帯域幅設定</p>	
<p>MC : 言語設定</p>	<p>AWI クライアント : 言語設定</p>	<p>OSD : 言語設定</p>
<p>MC : OSD 設定</p>	<p>AWI : OSD 設定</p>	<p>OSD : OSD 設定</p>
<p>MC : イメージ設定</p>	<p>AWI ホスト : イメージ設定 AWI クライアント : イメージ設 定</p>	<p>OSD : イメージ設定</p>
<p>MC : モニタエミュレーション</p>	<p>AWI Tera2 ホスト : モニタエミ ュレーション</p>	
<p>MC : 時間設定</p>	<p>AWI : 時間設定</p>	
<p>MC : セキュリティ設定</p>	<p>AWI : セキュリティ設定</p>	
<p>MC : オーディオ承認</p>	<p>AWI ホスト : オーディオ承認 AWI クライアント : オーディオ 承認</p>	

MC : 電源承認	AWI クライアント : 電源承認	
MC : ホストドライバ機能	AWI ホスト : ホストドライバ機能	
MC : イベントログ設定	AWI : イベントログ設定	OSD : イベントログ設定
MC : 周辺機器設定	AWI クライアント : 周辺機器設定	
MC : IPv6 設定	AWI : IPv6 設定	OSD : IPv6 設定
MC : ディスプレイトポロジ設定		OSD Tera2 : ディスプレイトポロジ設定
MC : OSD ログ設定	AWI クライアント : OSD ログ設定	
MC : フォームウェア管理	AWI : フォームウェアアップロード設定	
MC : USB 承認	AWI ホスト : USB 承認 AWI クライアント : USB 承認	
MC : 証明書ストア管理	AWI : 証明書アップロード設定	
MC : VMware View 証明書チェック設定	AWI : VMware View 証明書チェック設定	OSD : VMware View 証明書チェック設定

4.20 TERA1100 ゼロクライアントと VMware View 仮想デスクトップの接続

このトピックでは、第1世代 TERA1100 ゼロクライアントと VMware View 仮想デスクトップ間の接続の設定方法について説明します。

注意：使用されているゼロクライアントを特定するには、「[プロセッサ情報の表示](#)」を参照してください。このクライアントの表示オプションを確認するには、「[PCoIP ホストカードとゼロクライアント](#)」を参照してください。

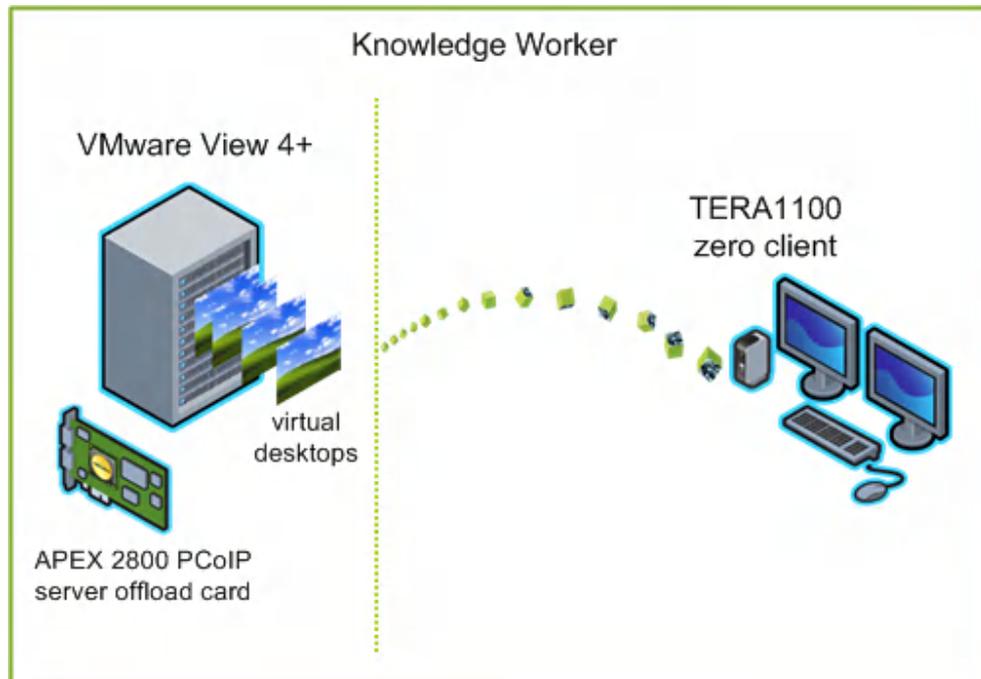


図 4-13 : TERA1100 ゼロクライアントと VMware View 仮想デスクトップの接続

図の左側は、一般的なサーバホスト型 VMware View 実装で、仮想デスクトップ（仮想デスクトップインフラストラクチャや VDI と呼ばれることもある）と APEX 2800 サーバオフロードカードのセットがハードウェア駆動型 PCoIP イメージエンコーディングを可能にします。右側のゼロクライアントは VMware View Connection Server ブローカを使用して VMware View 仮想デスクトップに接続しています。手動または自動ログオンを使用して、VMware View キオスクモード（デスクトップ上の情報に対する複数ユーザアクセスを提供する場合）を使用して、あるいは Imprivata OneSign テクノロジ（VDI ローミング実装で近接型カードをサポートする場合）を使用して VMware View 仮想デスクトップに接続するように設定することができます。これらの VMware View 設定オプションについては後述します。

注意：APEX 2800 の詳細については、『Teradici APEX 2800 Server Offload Card Administrator's Guide』（TER1109003）を参照してください。PCoIP ゼロクライアントと一緒に使用する場合の VMware View の設定方法については、『Using PCoIP Zero Clients with VMware View User Guide』（TER0904005）を参照してください。

4.21 前提条件

クライアントを VMware View 仮想デスクトップに接続する前に以下の条件をクリアする必要があります。

- VMware View Manager と VMware View Agent を含む VMware View インストールはバージョン 4.0.1 以降にする必要があります。詳細については、VMware のマ

マニュアルと『Using PCoIP Zero Clients with VMware View User Guide』
(TER0904005) を参照してください。

- ゼロクライアントのファームウェアバージョンは 3.1.0 以降にする必要があります。MC を使用したファームウェアのアップロード方法については、『PCoIP Management Console User Manual』 (TER0812002) を参照してください。MC を使用したプロファイルへのファームウェアファイルの割り当て方法については、『[MC : ファームウェア管理](#)』を参照してください。AWI を使用した単一ホストまたはクライアントへのファームウェアのアップロード方法については、『[AWI : ファームウェアアップロード設定](#)』を参照してください。
- ネットワークリソースは、帯域幅、QoS、遅延、ジッタ、およびパケットロスに関する要件を満たすことができる必要があります。PCoIP ネットワークアーキテクチャの設計方法については、『PC-over-IP Protocol Virtual Desktop Network Design Checklist』 (TER1105004) を参照してください。

4.22 セッション接続タイプ

PCoIP デプロイメントの規模によっては、管理コンソールを使用して VMware View セッション接続タイプを含むプロファイルを設定することも、AWI または OSD を使用して個別のゼロクライアントを VMware View セッション接続タイプを使用するように設定することもできます。

次の 4 つの接続オプションが使用できます。

- [View Connection Server](#)
- [View Connection Server + 自動ログオン](#)
- [View Connection Server + キオスク](#)
- [View Connection Server + Imprivata OneSign](#)

4.22.1 View Connection Server

クライアントを VMware 仮想デスクトップに接続するように設定するには、**View Connection Server** セッション接続タイプを使用します。このオプションの場合は、VMware View Connection Server の IP アドレス (または DNS 名) を指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : View Connection Server](#) : MC を使用してクライアントデバイスの **View Connection Server** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : View Connection Server](#) : AWI を使用して、クライアントを VMware View Connection Server 経由で仮想デスクトップに接続するための設定方法について説明します。

- [OSD : View Connection Server](#) : OSD を使用して、クライアントを VMware View Connection Server 経由で仮想デスクトップに接続するための設定方法について説明します。

4.22.2 View Connection Server + 自動ログオン

クライアントが仮想デスクトップに接続したときに自動的にユーザのログイン詳細を入力するように設定するには、**View Connection Server + 自動ログオンセッション** 接続タイプを使用します。VMware View Connection Server の IP アドレス（または DNS 名）の他に、ユーザ名、ユーザパスワード、およびサーバに送信するユーザのドメイン名も指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : View Connection Server + 自動ログオン](#) : MC を使用して、クライアントデバイスの **View Connection Server + 自動ログオンセッション** 接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : View Connection Server + 自動ログオン](#) : AWI を使用して、クライアントが VMware View Connection Server 経由で仮想デスクトップに接続したときに自動的にユーザのログイン詳細を入力するための設定方法について説明します。
- [OSD : View Connection Server + 自動ログオン](#) : OSD を使用して、クライアントが VMware View Connection Server 経由で仮想デスクトップに接続したときに自動的にユーザのログイン詳細を入力するための設定方法について説明します。

4.22.3 View Connection Server + キオスク

VMware View キオスクモードを使用すれば、複数のユーザがデスクトップに接続して個人情報以外の情報を入手する場合などに、キオスク実装に使用されるデスクトップに接続するようにクライアントを設定することができます。少なくとも、VMware View Connection Server の IP アドレス（または DNS 名）とキオスクユーザ名（キオスクのカスタムユーザ名または MAC アドレス）を指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : View Connection Server + キオスク](#) : MC を使用して、クライアントデバイスの **View Connection Server + Kiosk** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : View Connection Server + キオスク](#) : AWI を使用して、クライアントを VMware View Connection Server 経由で仮想デスクトップに接続するときにキオスクモードを使用するように設定する方法について説明します。
- [OSD : View Connection Server + キオスク](#) : OSD を使用して、クライアントを VMware View Connection Server 経由で仮想デスクトップに接続するときにキオスクモードを使用するように設定する方法について説明します。

4.22.4 View Connection Server + Imprivata OneSign

VMware View Imprivata OneSign モードを使用すれば、クライアントを VMware View Connection Server 経由で仮想デスクトップに接続するときに Imprivata OneSign 近接型カードを使用するように設定することができます。VMware View Connection Server の IP アドレス（または DNS 名）と OneSign サーバのブートストラップ URL を指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : View Connection Server + Imprivata OneSign](#) : MC を使用して、クライアントデバイスの **View Connection Server + Imprivata OneSign** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : View Connection Server + Imprivata OneSign](#) : AWI を使用して、クライアントを VMware View Connection Server 経由で仮想デスクトップに接続するときに Imprivata OneSign モードを使用するように設定する方法について説明します。
- [OSD : View Connection Server + Imprivata OneSign](#) : OSD を使用して、クライアントを VMware View Connection Server 経由で仮想デスクトップに接続するときに Imprivata OneSign モードを使用するように設定する方法について説明します。

4.22.5 その他の設定リンク

このセッションタイプに関するすべての範囲のファームウェアパラメータを設定するには、以下のトピックを参照してください。

注意 : OSD では一部の設定機能が使用できません。

MC を使用している場合	AWI を使用している場合	OSD を使用している場合
	AWI クライアント : 初期セットアップ	
MC : ネットワーク設定	AWI : ネットワーク設定	OSD : ネットワーク設定
MC を使用したデバイスネーミングの管理方法については、『PCoIP Management Console User Manual』(TER0812002) を参照してください。	AWI : ラベル設定	OSD : ラベル設定
MC : SNMP 設定	AWI : SNMP 設定	
MC : View Connection Server MC : View Connection Server	AWI クライアント : View Connection Server	OSD : View Connection Server OSD : View Connection Server

+ 自動ログオン MC : View Connection Server + キオスク MC : View Connection Server + Imprivata OneSign	AWI クライアント : View Connection Server + 自動ログオン AWI クライアント : View Connection Server + キオスク AWI クライアント : View Connection Server + Imprivata OneSign	+ 自動ログオン OSD : View Connection Server + キオスク OSD : View Connection Server + Imprivata OneSign
MC : 暗号化設定	AWI : 暗号化設定	
MC : 帯域幅設定	AWI : 帯域幅設定	
MC : 言語設定	AWI クライアント : 言語設定	OSD : 言語設定
MC : OSD 設定	AWI : OSD 設定	OSD : OSD 設定
MC : イメージ設定	AWI クライアント : イメージ設定	OSD : イメージ設定
MC : 時間設定	AWI : 時間設定	
MC : セキュリティ設定	AWI : セキュリティ設定	
MC : オーディオ承認	AWI クライアント : オーディオ承認	
MC : イベントログ設定	AWI : イベントログ設定	OSD : イベントログ設定
MC : 周辺機器設定	AWI クライアント : 周辺機器設定	
MC : IPv6 設定	AWI : IPv6 設定	OSD : IPv6 設定
MC : ディスプレイトポロジ設定		OSD Tera1 : ディスプレイトポロジ設定
MC : OSD ログ設定	AWI クライアント : OSD ログ設定	
MC : フォームウェア管理	AWI : フォームウェアアップロード設定	
MC : USB 承認	AWI クライアント : USB 承認	

MC : 証明書ストア管理	AWI : 証明書アップロード設定	
MC : VMware View 証明書チェック設定	AWI : VMware View 証明書チェック設定	OSD : VMware View 証明書チェック設定

4.23 TERA2321 ゼロクライアントと VMware View 仮想デスクトップの接続

このトピックでは、第2世代 TERA2321 ゼロクライアントと VMware View 仮想デスクトップ間の接続の設定方法について説明します。

注意：使用されているゼロクライアントを特定するには、「[プロセッサ情報の表示](#)」を参照してください。このクライアントの表示オプションを確認するには、「[PCoIP ホストカードとゼロクライアント](#)」を参照してください。

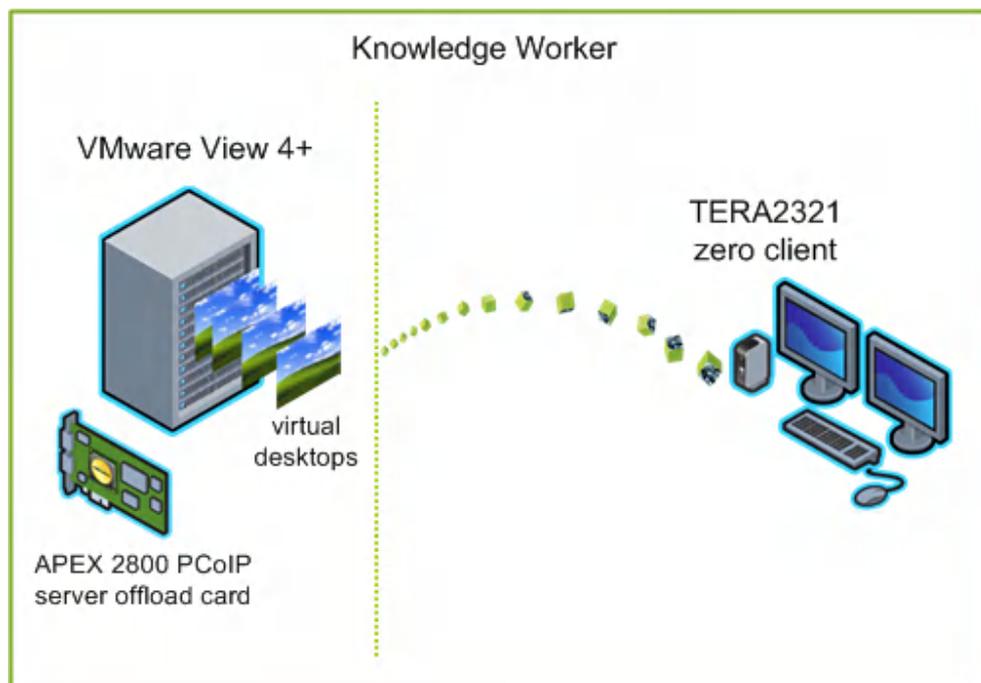


図 4-14 : TERA2321 ゼロクライアントと VMware View 仮想デスクトップの接続

図の左側は、一般的なサーバホスト型 VMware View 実装で、仮想デスクトップ（仮想デスクトップインフラストラクチャや VDI と呼ばれることもある）と APEX 2800 サーバオフロードカードのセットがハードウェア駆動型 PCoIP イメージエンコーディングを可能にします。右側のゼロクライアントは VMware View Connection Server ブローカを使用して VMware View 仮想デスクトップに接続しています。手動または自動ログオンを使用して、VMware View キオスクモード（デスクトップ上の情報に対する複数ユーザアクセスを提供する場合）を使用して、あるいは Imprivata OneSign テクノロジ（VDI ローミング実装で近接型カードをサポートする場合）を

使用して VMware View 仮想デスクトップに接続するように設定することができます。これらの VMware View 設定オプションについては後述します。

注意：APEX 2800 の詳細については、『[Teradici APEX 2800 Server Offload Card Administrator's Guide](#)』（TER1109003）を参照してください。PCoIP ゼロクライアントと一緒に使用する場合の VMware View の設定方法については、『[Using PCoIP Zero Clients with VMware View User Guide](#)』（TER0904005）を参照してください。

4.24 前提条件

クライアントを VMware View 仮想デスクトップに接続する前に以下の条件をクリアする必要があります。

- VMware View Manager と VMware View Agent を含む VMware View インストールはバージョン 4.0.1 以降にする必要があります。詳細については、VMware のマニュアルと『[Using PCoIP Zero Clients with VMware View User Guide](#)』（TER0904005）を参照してください。
- ゼロクライアントのファームウェアバージョンは 3.1.0 以降にする必要があります。MC を使用したファームウェアのアップロード方法については、『[PCoIP Management Console User Manual](#)』（TER0812002）を参照してください。MC を使用したプロファイルへのファームウェアファイルの割り当て方法については、『[MC：ファームウェア管理](#)』を参照してください。AWI を使用した単一ホストまたはクライアントへのファームウェアのアップロード方法については、『[AWI：ファームウェアアップロード設定](#)』を参照してください。
- ネットワークリソースは、帯域幅、QoS、遅延、ジッタ、およびパケットロスに関する要件を満たすことができる必要があります。PCoIP ネットワークアーキテクチャの設計方法については、『[PC-over-IP Protocol Virtual Desktop Network Design Checklist](#)』（TER1105004）を参照してください。

4.25 セッション接続タイプ

PCoIP デプロイメントの規模によっては、管理コンソールを使用して VMware View セッション接続タイプを含むプロファイルを設定することも、AWI または OSD を使用して個別のゼロクライアントを VMware View セッション接続タイプを使用するように設定することもできます。

次の 4 つの接続オプションが使用できます。

- [View Connection Server](#)
- [View Connection Server + 自動ログオン](#)
- [View Connection Server + キオスク](#)
- [View Connection Server + Imprivata OneSign](#)

4.25.1 View Connection Server

クライアントを VMware 仮想デスクトップに接続するように設定するには、**View Connection Server** セッション接続タイプを使用します。このオプションの場合は、VMware View Connection Server の IP アドレス（または DNS 名）を指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : View Connection Server](#) : MC を使用してクライアントデバイスの **View Connection Server** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : View Connection Server](#) : AWI を使用して、クライアントを VMware View Connection Server 経由で仮想デスクトップに接続するための設定方法について説明します。
- [OSD : View Connection Server](#) : OSD を使用して、クライアントを VMware View Connection Server 経由で仮想デスクトップに接続するための設定方法について説明します。

4.25.2 View Connection Server + 自動ログオン

クライアントが仮想デスクトップに接続したときに自動的にユーザのログイン詳細を入力するように設定するには、**View Connection Server + 自動ログオン** セッション接続タイプを使用します。VMware View Connection Server の IP アドレス（または DNS 名）の他に、ユーザ名、ユーザパスワード、およびサーバに送信するユーザのドメイン名も指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : View Connection Server + 自動ログオン](#) : MC を使用して、クライアントデバイスの **View Connection Server + 自動ログオン** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : View Connection Server + 自動ログオン](#) : AWI を使用して、クライアントが VMware View Connection Server 経由で仮想デスクトップに接続したときに自動的にユーザのログイン詳細を入力するための設定方法について説明します。
- [OSD : View Connection Server + 自動ログオン](#) : OSD を使用して、クライアントが VMware View Connection Server 経由で仮想デスクトップに接続したときに自動的にユーザのログイン詳細を入力するための設定方法について説明します。

4.25.3 View Connection Server + キオスク

VMware View キオスクモードを使用すれば、複数のユーザがデスクトップに接続して個人情報以外の情報を入手する場合などに、キオスク実装に使用されるデスクトップに接続するようにクライアントを設定することができます。少なくとも、

VMware View Connection Server の IP アドレス（または DNS 名）とキオスクユーザ名（キオスクのカスタムユーザ名または MAC アドレス）を指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : View Connection Server + キオスク](#) : MC を使用して、クライアントデバイスの **View Connection Server + Kiosk** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : View Connection Server + キオスク](#) : AWI を使用して、クライアントを VMware View Connection Server 経由で仮想デスクトップに接続するときにキオスクモードを使用するように設定する方法について説明します。
- [OSD : View Connection Server + キオスク](#) : OSD を使用して、クライアントを VMware View Connection Server 経由で仮想デスクトップに接続するときにキオスクモードを使用するように設定する方法について説明します。

4.25.4 View Connection Server + Imprivata OneSign

VMware View Imprivata OneSign モードを使用すれば、クライアントを VMware View Connection Server 経由で仮想デスクトップに接続するときに Imprivata OneSign 近接型カードを使用するように設定することができます。VMware View Connection Server の IP アドレス（または DNS 名）と OneSign サーバのブートストラップ URL を指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : View Connection Server + Imprivata OneSign](#) : MC を使用して、クライアントデバイスの **View Connection Server + Imprivata OneSign** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : View Connection Server + Imprivata OneSign](#) : AWI を使用して、クライアントを VMware View Connection Server 経由で仮想デスクトップに接続するときに Imprivata OneSign モードを使用するように設定する方法について説明します。
- [OSD : View Connection Server + Imprivata OneSign](#) : OSD を使用して、クライアントを VMware View Connection Server 経由で仮想デスクトップに接続するときに Imprivata OneSign モードを使用するように設定する方法について説明します。

4.25.5 その他の設定リンク

このセッションタイプに関するすべての範囲のファームウェアパラメータを設定するには、以下のトピックを参照してください。

注意 : OSD では一部の設定機能が使用できません。

注意：TERA2321 ゼロクライアントには第1世代 TERA1100 クライアントと同じディスプレイポロジがあります。このことは、このセクション内のディスプレイポロジページへのリンクに反映されています。

MC を使用している場合	AWI を使用している場合	OSD を使用している場合
	AWI クライアント：初期セットアップ	
MC：ネットワーク設定	AWI：ネットワーク設定	OSD：ネットワーク設定
MC を使用したデバイスネーミングの管理方法については、『PCoIP Management Console User Manual』（TER0812002）を参照してください。	AWI：ラベル設定	OSD：ラベル設定
MC：SNMP 設定	AWI：SNMP 設定	
MC：View Connection Server MC：View Connection Server + 自動ログオン MC：View Connection Server + キオスク MC：View Connection Server + Imprivata OneSign	AWI クライアント：View Connection Server AWI クライアント：View Connection Server + 自動ログオン AWI クライアント：View Connection Server + キオスク AWI クライアント：View Connection Server + Imprivata OneSign	OSD：View Connection Server OSD：View Connection Server + 自動ログオン OSD：View Connection Server + キオスク OSD：View Connection Server + Imprivata OneSign
MC：暗号化設定	AWI：暗号化設定	
MC：帯域幅設定	AWI：帯域幅設定	
MC：言語設定	AWI クライアント：言語設定	OSD：言語設定
MC：OSD 設定	AWI：OSD 設定	OSD：OSD 設定
MC：イメージ設定	AWI クライアント：イメージ設定	OSD：イメージ設定
MC：時間設定	AWI：時間設定	
MC：セキュリティ設定	AWI：セキュリティ設定	

MC : オーディオ承認	AWI クライアント : オーディオ承認	
MC : イベントログ設定	AWI : イベントログ設定	OSD : イベントログ設定
MC : 周辺機器設定	AWI クライアント : 周辺機器設定	
MC : IPv6 設定	AWI : IPv6 設定	OSD : IPv6 設定
MC : ディスプレイトボログ設定		OSD Tera1 : ディスプレイトボログ設定
MC : OSD ログ設定	AWI クライアント : OSD ログ設定	
MC : フォームウェア管理	AWI : フォームウェアアップロード設定	
MC : USB 承認	AWI クライアント : USB 承認	
MC : 証明書ストア管理	AWI : 証明書アップロード設定	
MC : VMware View 証明書チェック設定	AWI : VMware View 証明書チェック設定	OSD : VMware View 証明書チェック設定

4.26 TERA2140 ゼロクライアントと VMware View 仮想デスクトップの接続

このトピックでは、第2世代 TERA2140 ゼロクライアントと VMware View 仮想デスクトップ間の接続の設定方法について説明します。

注意：使用されているゼロクライアントを特定するには、「[プロセッサ情報の表示](#)」を参照してください。このクライアントの表示オプションを確認するには、「[PCoIP ホストカードとゼロクライアント](#)」を参照してください。

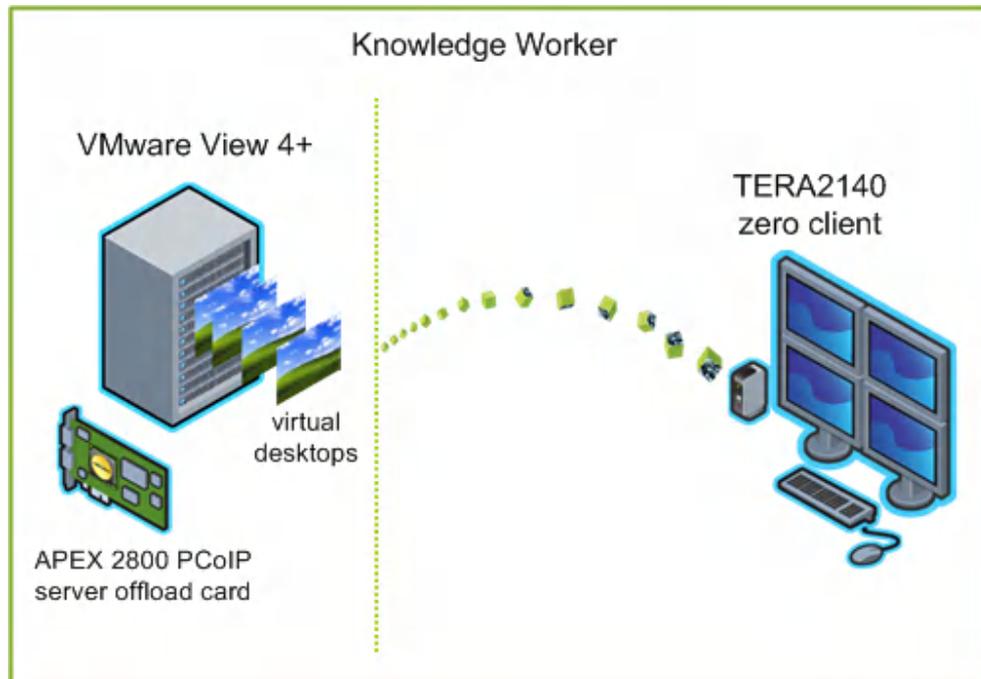


図 4-15 : TERA2140 ゼロクライアントと VMware View 仮想デスクトップの接続

図の左側は、一般的なサーバホスト型 VMware View 実装で、仮想デスクトップ（仮想デスクトップインフラストラクチャや VDI と呼ばれることもある）と APEX 2800 サーバオフロードカードのセットがハードウェア駆動型 PCoIP イメージエンコーディングを可能にします。右側のゼロクライアントは VMware View Connection Server ブローカを使用して VMware View 仮想デスクトップに接続しています。手動または自動ログオンを使用して、VMware View キオスクモード（デスクトップ上の情報に対する複数ユーザアクセスを提供する場合）を使用して、あるいは Imprivata OneSign テクノロジ（VDI ローミング実装で近接型カードをサポートする場合）を使用して VMware View 仮想デスクトップに接続するように設定することができます。これらの VMware View 設定オプションについては後述します。

注意：APEX 2800 の詳細については、『Teradici APEX 2800 Server Offload Card Administrator's Guide』（TER1109003）を参照してください。PCoIP ゼロクライアントと一緒に使用する場合の VMware View の設定方法については、『Using PCoIP Zero Clients with VMware View User Guide』（TER0904005）を参照してください。

4.27 前提条件

クライアントを VMware View 仮想デスクトップに接続する前に以下の条件をクリアする必要があります。

- VMware View Manager と VMware View Agent を含む VMware View インストールはバージョン 4.0.1 以降にする必要があります。詳細については、VMware のマ

マニュアルと『Using PCoIP Zero Clients with VMware View User Guide』
(TER0904005)を参照してください。

- ゼロクライアントのファームウェアバージョンは3.1.0以降にする必要があります。MCを使用したファームウェアのアップロード方法については、『PCoIP Management Console User Manual』(TER0812002)を参照してください。MCを使用したプロファイルへのファームウェアファイルの割り当て方法については、「[MC：ファームウェア管理](#)」を参照してください。AWIを使用した単一ホストまたはクライアントへのファームウェアのアップロード方法については、「[AWI：ファームウェアアップロード設定](#)」を参照してください。
- ネットワークリソースは、帯域幅、QoS、遅延、ジッタ、およびパケットロスに関する要件を満たすことができる必要があります。PCoIP ネットワークアーキテクチャの設計方法については、『PC-over-IP Protocol Virtual Desktop Network Design Checklist』(TER1105004)を参照してください。

4.28 セッション接続タイプ

PCoIP デプロイメントの規模によっては、管理コンソールを使用して VMware View セッション接続タイプを含むプロファイルを設定することも、AWI または OSD を使用して個別のゼロクライアントを VMware View セッション接続タイプを使用するように設定することもできます。

次の4つの接続オプションが使用できます。

- [View Connection Server](#)
- [View Connection Server + 自動ログオン](#)
- [View Connection Server + キオスク](#)
- [View Connection Server + Imprivata OneSign](#)

4.28.1 View Connection Server

クライアントを VMware 仮想デスクトップに接続するように設定するには、**View Connection Server** セッション接続タイプを使用します。このオプションの場合は、VMware View Connection Server の IP アドレス (または DNS 名) を指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC：View Connection Server](#)：MC を使用してクライアントデバイスの **View Connection Server** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント：View Connection Server](#)：AWI を使用して、クライアントを VMware View Connection Server 経由で仮想デスクトップに接続するための設定方法について説明します。

- [OSD : View Connection Server](#) : OSD を使用して、クライアントを VMware View Connection Server 経由で仮想デスクトップに接続するための設定方法について説明します。

4.28.2 View Connection Server + 自動ログオン

クライアントが仮想デスクトップに接続したときに自動的にユーザのログイン詳細を入力するように設定するには、**View Connection Server + 自動ログオンセッション** 接続タイプを使用します。VMware View Connection Server の IP アドレス（または DNS 名）の他に、ユーザ名、ユーザパスワード、およびサーバに送信するユーザのドメイン名も指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : View Connection Server + 自動ログオン](#) : MC を使用して、クライアントデバイスの **View Connection Server + 自動ログオンセッション** 接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : View Connection Server + 自動ログオン](#) : AWI を使用して、クライアントが VMware View Connection Server 経由で仮想デスクトップに接続したときに自動的にユーザのログイン詳細を入力するための設定方法について説明します。
- [OSD : View Connection Server + 自動ログオン](#) : OSD を使用して、クライアントが VMware View Connection Server 経由で仮想デスクトップに接続したときに自動的にユーザのログイン詳細を入力するための設定方法について説明します。

4.28.3 View Connection Server + キオスク

VMware View キオスクモードを使用すれば、複数のユーザがデスクトップに接続して個人情報以外の情報を入手する場合などに、キオスク実装に使用されるデスクトップに接続するようにクライアントを設定することができます。少なくとも、VMware View Connection Server の IP アドレス（または DNS 名）とキオスクユーザ名（キオスクのカスタムユーザ名または MAC アドレス）を指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : View Connection Server + キオスク](#) : MC を使用して、クライアントデバイスの **View Connection Server + Kiosk** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : View Connection Server + キオスク](#) : AWI を使用して、クライアントを VMware View Connection Server 経由で仮想デスクトップに接続するときにキオスクモードを使用するように設定する方法について説明します。
- [OSD : View Connection Server + キオスク](#) : OSD を使用して、クライアントを VMware View Connection Server 経由で仮想デスクトップに接続するときにキオスクモードを使用するように設定する方法について説明します。

4.28.4 View Connection Server + Imprivata OneSign

VMware View Imprivata OneSign モードを使用すれば、クライアントを VMware View Connection Server 経由で仮想デスクトップに接続するときに Imprivata OneSign 近接型カードを使用するように設定することができます。VMware View Connection Server の IP アドレス（または DNS 名）と OneSign サーバのブートストラップ URL を指定する必要があります。

このオプションの設定方法については、GUI リファレンス内の以下のトピックを参照してください。

- [MC : View Connection Server + Imprivata OneSign](#) : MC を使用して、クライアントデバイスの **View Connection Server + Imprivata OneSign** セッション接続タイプを定義したプロファイルを設定する方法について説明します。
- [AWI クライアント : View Connection Server + Imprivata OneSign](#) : AWI を使用して、クライアントを VMware View Connection Server 経由で仮想デスクトップに接続するときに Imprivata OneSign モードを使用するように設定する方法について説明します。
- [OSD : View Connection Server + Imprivata OneSign](#) : OSD を使用して、クライアントを VMware View Connection Server 経由で仮想デスクトップに接続するときに Imprivata OneSign モードを使用するように設定する方法について説明します。

4.28.5 その他の設定リンク

このセッションタイプに関するすべての範囲のファームウェアパラメータを設定するには、以下のトピックを参照してください。

注意 : OSD では一部の設定機能が使用できません。

MC を使用している場合	AWI を使用している場合	OSD を使用している場合
	AWI クライアント : 初期セットアップ	
MC : ネットワーク設定	AWI : ネットワーク設定	OSD : ネットワーク設定
MC を使用したデバイスネーミングの管理方法については、『PCoIP Management Console User Manual』（TER0812002）を参照してください。	AWI : ラベル設定	OSD : ラベル設定
MC : SNMP 設定	AWI : SNMP 設定	
MC : View Connection Server MC : View Connection Server +	AWI クライアント : View Connection Server	OSD : View Connection Server OSD : View Connection Server

自動ログオン MC : View Connection Server + キオスク MC : View Connection Server + Imprivata OneSign	AWI クライアント : View Connection Server + 自動ログオン AWI クライアント : View Connection Server + キオスク AWI クライアント : View Connection Server + Imprivata OneSign	+ 自動ログオン OSD : View Connection Server + キオスク OSD : View Connection Server + Imprivata OneSign
MC : 暗号化設定	AWI : 暗号化設定	
MC : 帯域幅設定	AWI : 帯域幅設定	
MC : 言語設定	AWI クライアント : 言語設定	OSD : 言語設定
MC : OSD 設定	AWI : OSD 設定	OSD : OSD 設定
MC : イメージ設定	AWI クライアント : イメージ設定	OSD : イメージ設定
MC : 時間設定	AWI : 時間設定	
MC : セキュリティ設定	AWI : セキュリティ設定	
MC : オーディオ承認	AWI クライアント : オーディオ承認	
MC : イベントログ設定	AWI : イベントログ設定	OSD : イベントログ設定
MC : 周辺機器設定	AWI クライアント : 周辺機器設定	
MC : IPv6 設定	AWI : IPv6 設定	OSD : IPv6 設定
MC : ディスプレイポートロジ設定		OSD Tera2 : ディスプレイポートロジ設定
MC : OSD ログ設定	AWI クライアント : OSD ログ設定	
MC : フォームウェア管理	AWI : フォームウェアアップロード設定	
MC : USB 承認	AWI クライアント : USB 承認	

MC : 証明書ストア管理	AWI : 証明書アップロード設定	
MC : VMware View 証明書チェック設定	AWI : VMware View 証明書チェック設定	OSD : VMware View 証明書チェック設定

4.29 VMware View クライアントと VMware View 仮想デスクトップの接続

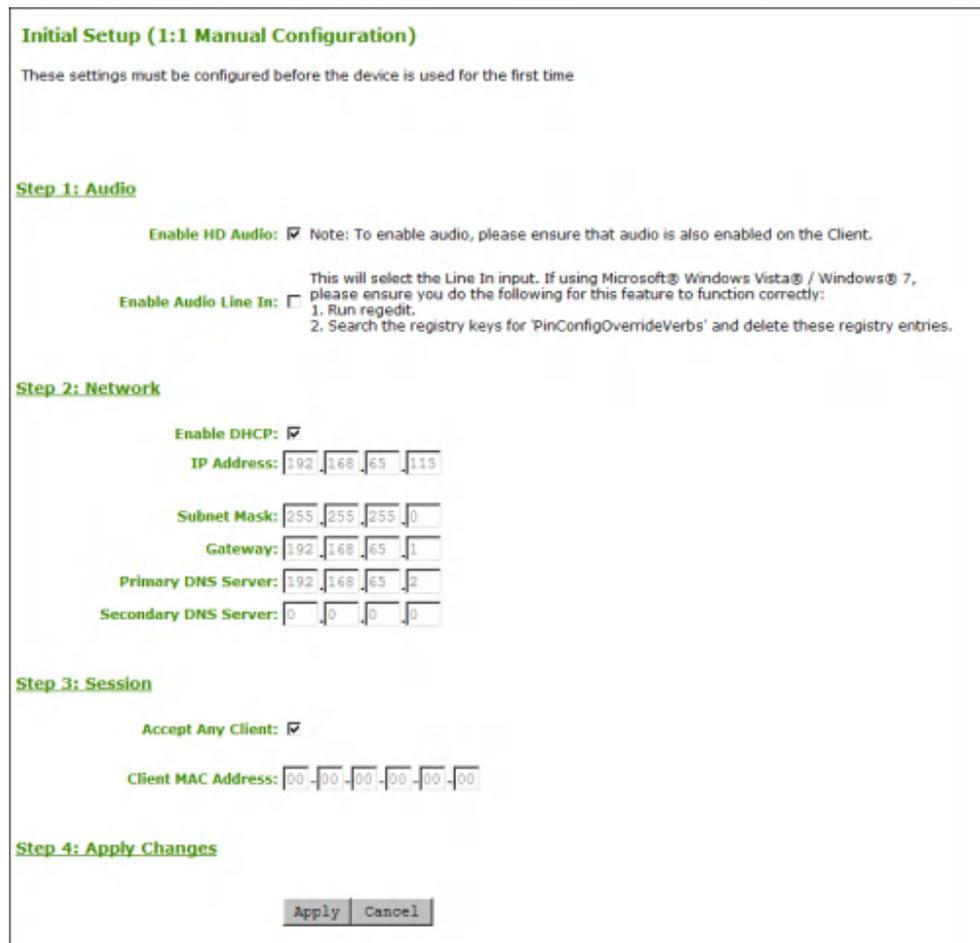
PC、ラップトップ、電話機、またはモバイルプラットフォームにインストールされた VMware View 4 以降のソフトウェアクライアント経由で VMware View 仮想デスクトップに接続することにより、PCoIP プロトコルテクノロジーを利用することもできます。この VMware View VDI ソリューションをインストールして管理する方法については、VMware View のマニュアルを参照してください。

5 PCoIP GUI リファレンス

5.1 初期セットアップ

5.1.1 AWI ホスト : Initial Setup ページ

このページは、**Configuration > Initial Setup** メニューから表示することができます。



Initial Setup (1:1 Manual Configuration)

These settings must be configured before the device is used for the first time

Step 1: Audio

Enable HD Audio: Note: To enable audio, please ensure that audio is also enabled on the Client.

Enable Audio Line In: This will select the Line In input. If using Microsoft® Windows Vista® / Windows® 7, please ensure you do the following for this feature to function correctly:
 1. Run regedit.
 2. Search the registry keys for 'PinConfigOverrideVerbs' and delete these registry entries.

Step 2: Network

Enable DHCP:

IP Address: 192 . 168 . 65 . 115

Subnet Mask: 255 . 255 . 255 . 0

Gateway: 192 . 168 . 65 . 1

Primary DNS Server: 192 . 168 . 65 . 2

Secondary DNS Server: 0 . 0 . 0 . 0

Step 3: Session

Accept Any Client:

Client MAC Address: 00 - 00 - 00 - 00 - 00 - 00

Step 4: Apply Changes

Apply Cancel

図 5-1 : AWI ホスト Initial Setup ページ

表 5-1 : オーディオパラメータ

パラメータ	説明
Enable HD Audio	ホストまたはクライアント上でのオーディオサポートを有効にします。

パラメータ	説明
Enable Microsoft® Windows Vista® 64-bit Mode	<p>ホスト上で 64 ビットモードを有効にします。このモードは Windows Vista 64 ビットバージョンと Windows 7® 64 ビットバージョン以外では使用しないでください。オーディオ機能が正常に動作しない可能性があります。</p> <p>注意：Linux、Windows 7® 32 ビット、Windows Vista 32 ビット、または Windows XP (32 ビットまたは 64 ビット) では、64 ビットモードを有効にする必要がありません。</p>
Enable Audio Line In	<p>有効化：クライアント上で発見されたライン入力コネクタが使用されます。</p> <p>無効化：ライン入力コネクタがマイクロホン入力として使用されます。</p> <p>デバイス上に Windows Vista または Windows 7 がインストールされている場合は、画面上の指示に従ってください。</p>

表 5-2：ネットワークパラメータ

パラメータ	説明
Enable DHCP	DHCP を有効にします (手動 IP アドレス設定を使用する場合は対照的)。
IP Address	デバイスの IP アドレス
Subnet Mask	デバイスのサブネットマスク
Gateway	デバイスのゲートウェイ IP アドレス
Primary DNS Server	デバイスのプライマリ DNS IP アドレス
Secondary DNS Server	デバイスのセカンダリ DNS IP アドレス

表 5-3：セッションパラメータ

パラメータ	説明
Accept Any Client	ホストが任意のクライアントからの PCoIP セッションを受け入れるようにします。
Client MAC Address	<p>PCoIP セッションのクライアント MAC アドレスを指定できるようにします。</p> <p>注意：クライアント MAC アドレスを 00-00-00-00-00-00 に設定することはできません。</p>

5.1.2 AWI クライアント : Initial Setup ページ

このページは、**Configuration > Initial Setup** メニューから表示することができます。

Initial Setup (1:1 Manual Configuration)

These settings must be configured before the device is used for the first time

Step 1: Audio

Enable HD Audio: Note: To enable audio, please ensure that audio is also enabled on the Host.

Step 2: Network

Enable DHCP:

IP Address:

Subnet Mask:

Gateway:

Primary DNS Server:

Secondary DNS Server:

Step 3: Session

Identify Host by: IP address FQDN

Host IP Address:

Host MAC Address:

Step 4: Apply Changes

図 5-2 : AWI クライアント Initial Setup ページ

表 5-4 : オーディオパラメータ

パラメータ	説明
Enable HD Audio	ホストまたはクライアント上でのオーディオサポートを有効にします。

表 5-5 : ネットワークパラメータ

パラメータ	説明
Enable DHCP	DHCP を有効にします (手動 IP アドレス設定を使用する場合とは対照的)。

パラメータ	説明
IP Address	デバイスの IP アドレス
Subnet Mask	デバイスのサブネットマスク
Gateway	デバイスのゲートウェイ IP アドレス
Primary DNS Server	デバイスのプライマリ DNS IP アドレス
Secondary DNS Server	デバイスのセカンダリ DNS IP アドレス

表 5-6 : セッションパラメータ

パラメータ	説明
Identify Host By	ホスト識別方法を指定します。
Host IP Address	ホスト IP アドレスを指定します。
Host MAC Address	ホスト MAC アドレスを指定します。 ホスト MAC アドレスを 00-00-00-00-00-00 に設定してセッション開始時にこのフィールドを無視することができます。

注意：クライアント上でホストディスカバリまたは接続管理が設定されている場合は、クライアントセッションパラメータを変更することができません。セッションパラメータの代わりにメッセージが **Initial Setup Client** ページに表示されます。

5.2 ネットワークの設定

5.2.1 MC : ネットワーク設定

このページの設定を使用すれば、動的ホスト構成プロトコル (DHCP) 、最大転送単位 (MTU) 、およびシンプルネットワークマネジメントプロトコルの各パラメータを使用してプロファイルを構成することができます。

MC でプロパティを有効にするには、**Set in Profile** チェックボックスをオンにし、指示に従ってフィールドを設定します。このページでプロパティを更新したら、**Save** をクリックして変更を保存します。

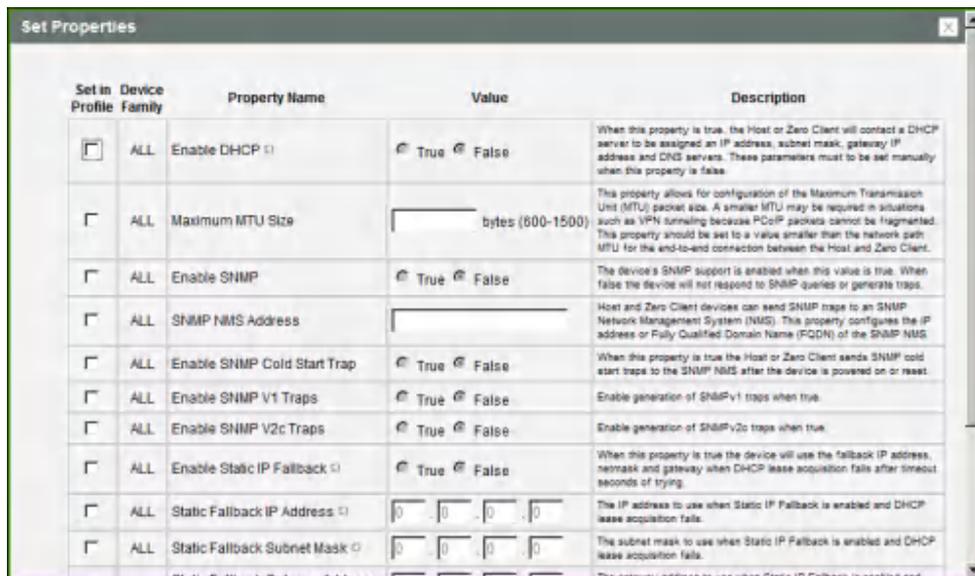


図 5-3 : MC ネットワーク設定

表 5-7 : MC ネットワーク設定パラメータ

パラメータ	説明
Enable DHCP	<p>有効になっている場合は、デバイスが DHCP サーバに IP アドレス、サブネットマスク、ゲートウェイ IP アドレス、および DNS サーバを割り当てるように指示し、ドメイン名 (オプション 15)、ホスト名 (オプション 12)、およびクライアント完全修飾ドメイン名 (FQDN) も要求します。</p> <p>無効になっている場合は、これらのパラメータを手動で設定する必要があります。</p> <p>注意 : MC ディスカバリの場合は、デバイスがベンダクラスオプション 60/43 も要求します。</p> <p>注意 : このプロパティを変更した場合はデバイスを再起動する必要があります。</p>
Maximum MTU Size	<p>最大転送単位 パケットサイズを設定することができます。</p> <p>PCoIP パケットはフラグメント化することができないため、VPN トンネリングなどの状況では、MTU を小さくする必要があります。ホストとクライアント間のエンドツーエンド接続では、Maximum MTU Size をネットワークパス MTU よりも小さな値に設定します。</p> <p>Maximum MTU Size の範囲は、すべてのファームウェアバージョンで 600~1500 バイトです。</p> <p>注意 : PCoIP ゼロクライアントと PCoIP ホストカード間のセッションのデフォルト MTU は 1400 です。</p> <p>VMware View などの PCoIP ソフトウェア (ホストまたはクライアント上) のデフォルト MTU は 1300 です。</p>

パラメータ	説明
Enable SNMP	有効になっている場合は、デバイスが PCoIP SNMP エージェントから SNMP 要求に応答できるようにします。SNMP エージェントを無効にすると、SNMP 要求に応答することも、トラップを生成することもできなくなります。また、PCoIP SNMP MIB にアクセスすることもできなくなります。
SNMP NMS Address	デバイスから SNMP ネットワーク管理システム (NMS) に SNMP トラップを送信したい場合は、SNMP NMS の IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。
Enable SNMP Cold Start Trap	有効になっている場合は、デバイスが電源投入後またはリセット後に SNMP NMS に SNMP コールドスタートトラップを送信します。
Enable SNMP V1 Traps	有効になっている場合は、SNMPv1 トラップの生成が可能になります。
Enable SNMP V2c Traps	有効になっている場合は、SNMPv2c トラップの生成が可能になります。
Enable Static IP Fallback	有効になっている場合は、デバイスが、試行のタイムアウト時間が経過して DHCP リースの取得に失敗したときに、フォールバック IP アドレス、ネットマスク、およびゲートウェイを使用します。 注意：このプロパティを変更した場合はデバイスを再起動する必要があります。
Static Fallback IP Address	Static IP Fallback が有効で DHCP リースの取得に失敗した場合に使用する IP アドレスを設定します。 注意：このプロパティを変更した場合はデバイスを再起動する必要があります。
Static Fallback Subnet Mask	Static IP Fallback が有効で DHCP リースの取得に失敗した場合に使用するサブネットマスクを設定します。 注意：このプロパティを変更した場合はデバイスを再起動する必要があります。
Static Fallback Gateway Address	Static IP Fallback が有効で DHCP リースの取得に失敗した場合に使用するゲートウェイアドレスを設定します。 注意：このプロパティを変更した場合はデバイスを再起動する必要があります。
Static Fallback Timeout	デバイスがフォールバックアドレス設定を使用する前に DHCP リースの取得を試みる時間を秒単位で設定します。60 以上の値を入力する必要があります。

パラメータ	説明
	<p>注意：フォールバック設定がアクティブになるまでに、この値よりもさらに最大 30 秒 長くなる場合があります。</p> <p>注意：このプロパティを変更した場合はデバイスを再起動する必要があります。</p>
SNMP Community Name	デバイスで使用される SNMP コミュニティ名を設定します。

5.2.2 AWI : ネットワーク設定

このページでは、ホストまたはクライアントのネットワーク設定を構成することができます。このページは、**Configuration > Network** メニューから表示することができます。このページでパラメータを更新したら、**Apply** をクリックして変更を保存します。

注意：ホストの [Initial Setup](#) ページとクライアントの [Initial Setup](#) ページからもネットワーク情報を設定することができます。

Network

Change the network settings for the device

Enable DHCP:

IP Address:

Subnet Mask:

Gateway:

Primary DNS Server:

Secondary DNS Server:

Domain Name:

FQDN:

Ethernet Mode:

Maximum MTU Size: bytes

Enable 802.1X Security:

Authentication:

Identity:

Client Certificate:

図 5-4 : AWI Network ページ

表 5-8 : AWI Network ページパラメータ

パラメータ	説明
Enable DHCP	有効になっている場合は、デバイスが DHCP サーバに IP アドレス、サブネットマスク、ゲートウェイ IP アドレス、および DNS サーバを割り当てるように指示し、ドメイン名 (オプション 15)、ホスト名 (オプション 12)、およびクライアント完全修飾ドメイン名 (FQDN) も要求します。 無効になっている場合は、これらのパラメータを手動で設定する必要があります。
IP Address	デバイスの IP アドレス。DHCP が無効になっている場合は、このフィールドを有効な IP アドレスに設定する必要があります。DHCP が有効になっている場合は、このフィールドを編集することができません。
Subnet Mask	デバイスのサブネットマスク。DHCP が無効になっている場合は、このフィールドを有効なサブネットマスクに設定する必要があります。DHCP が有効になっている場合は、このフィールドを編集することができません。 警告：不正な IP アドレス/サブネットマスクの組み合わせ (無効なマスクなど) を設定すると、デバイスにアクセスできなくなる可能性があります。サブネットマスクの設定は慎重に行ってください。
Gateway	デバイスのゲートウェイ IP アドレス。DHCP が無効になっている場合は、このフィールドが必須です。DHCP が有効になっている場合は、このフィールドを編集することができません。
Primary DNS Server	デバイスのプライマリ DNS IP アドレス。このフィールドは省略可能です。コネクションマネージャの使用中に DNS サーバの IP アドレスが設定された場合は、コネクションマネージャアドレスを IP アドレスの代わりに FQDN として設定することができます。
Secondary DNS Server	デバイスのセカンダリ DNS IP アドレス。このフィールドは省略可能です。コネクションマネージャの使用中に DNS サーバの IP アドレスが設定された場合は、コネクションマネージャアドレスを IP アドレスの代わりに FQDN として設定することができます。
Domain Name	ホストまたはクライアントのドメイン名 ("domain.local"など)。このフィールドは省略可能です。
FQDN	ホストまたはクライアントの完全修飾ドメイン名。デフォルトは pcoip-host-<MAC>または pcoip-portal-<MAC>です。ここで、<MAC>はホストまたはクライアントの MAC アドレスです。使用された場合はドメイン名が付加されます (pcoip-host-<MAC>.domain.local など)。このページのこのフィールドは読み取り専用です。 注意：FQDN 機能を使用するには、DHCP オプション 81 を使用した

パラメータ	説明
	DNS サーバを用意して正しく設定する必要があります。
Ethernet Mode	<p>次のようにホストまたはクライアントのイーサネットモードを設定することができます。</p> <ul style="list-style-type: none"> • Auto • 100 Mbps Full-Duplex • 10 Mbps Full-Duplex <p>10 Mbps Full Duplex または 100 Mbps Full-Duplex を選択してから Apply をクリックすると、次の警告メッセージが表示されます。</p> <p>「Warning : When Auto-Negotiation is disabled on the PCoIP device, it must also be disabled on the switch. Additionally, the PCoIP device and switch must be configured to use the same speed and duplex parameters. Different parameters may result in a loss of network connectivity. Are you sure you want to continue?」</p> <p>パラメータを変更する場合は OK をクリックします。</p> <p>注意：他のネットワーク機器（スイッチなど）も 10 Mbps 全二重 または 100 Mbps 全二重 で動作するように設定されている場合は、必ず、イーサネットモードを Auto に設定し、10 Mbps Full-Duplex または 100 Mbps Full-Duplex 以外を使用しないようにする必要があります。イーサネットモードの設定が不適切な場合は、ネットワーク動作が PCoIP プロトコルでサポートされていない半二重になる可能性があります。セッションの品質が極端に低下して、最終的に停止します。</p>
Maximum MTU Size	<p>最大転送単位 パケットサイズを設定することができます。</p> <p>PCoIP パケットはフラグメント化することができないため、VPN トンネリングなどの状況では、MTU を小さくする必要があります。ホストとクライアント間のエンドツーエンド接続では、Maximum MTU Size をネットワークパス MTU よりも小さな値に設定します。</p> <p>Maximum MTU Size の範囲は、すべてのファームウェアバージョンで 600～1500 バイトです。</p> <p>注意：PCoIP ゼロクライアントと PCoIP ホストカード間のセッションのデフォルト MTU は 1400 です。</p> <p>VMware View などの PCoIP ソフトウェア（ホストまたはクライアント上）のデフォルト MTU は 1300 です。</p>
Enable 802.1X Security	<p>ネットワークで 802.1X セキュリティが使用されている場合は、すべてのホストとゼロクライアントのこのフィールドを有効にします。有効になっている場合は、Authentication フィールド、Identity フィールド、および Client Certificate フィールドを設定します。</p>
Authentication	<p>このフィールドは TLS（トランスポート層セキュリティ）に設定され、グレーアウトされています。TLS が現時点でサポートされている唯一の認証プロトコルです。</p>

パラメータ	説明
Identity	ネットワーク上でデバイスを識別するための識別文字列を入力します。
Client Certificate	<p>Choose をクリックして 802.1X デバイスに使用するクライアント証明書を選択します。表示された証明書のリストには、Certificate Upload ページからアップロードされた、秘密鍵を含む証明書が含まれています。Network ページで選択した証明書は、Certificate Upload ページの読み取り専用 Client Certificate フィールドにリンクされています。</p> <p>注意：PCoIP は 1 つの 802.1X クライアント証明書しかサポートしていません。セキュリティ詳細のすべてが 1 つのファイルに含まれていることを確認してください。802.1X 証明書には秘密鍵が含まれている必要があります。</p>

5.2.3 OSD : ネットワーク設定

このページでは、クライアントのネットワーク設定を構成することができます。このページは、**Options > Configuration > Network** メニューから表示することができます。このページでパラメータを更新したら、**Apply** をクリックして変更を保存します。

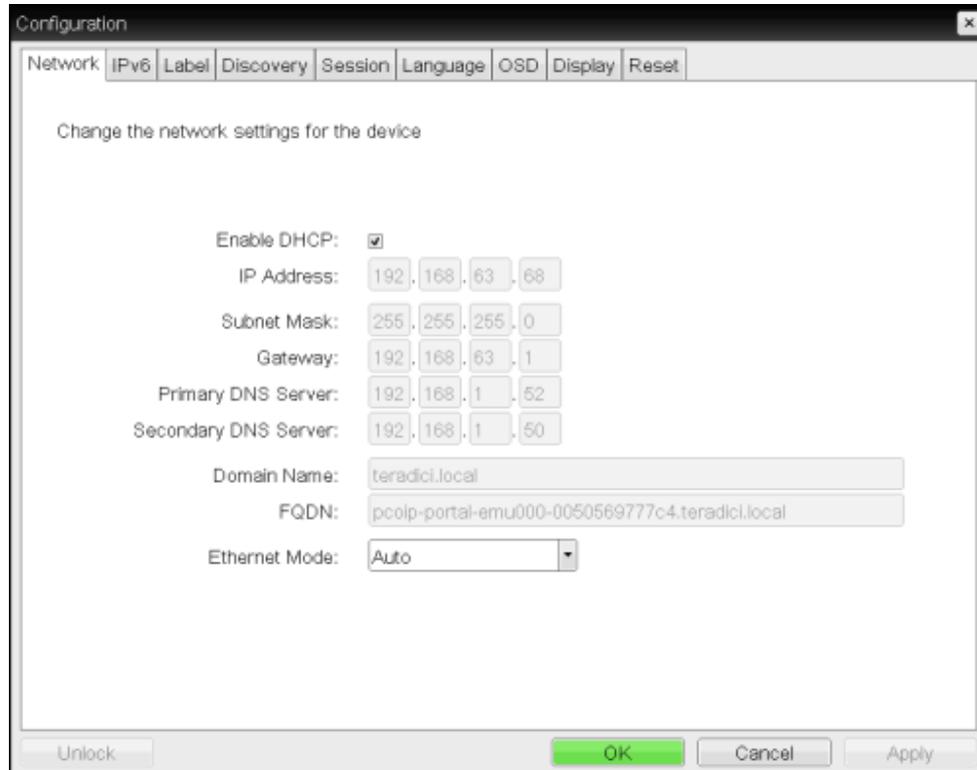


図 5-5 : OSD Network ページ

表 5-9 : OSD Network ページパラメータ

パラメータ	説明
Enable DHCP	<p>有効になっている場合は、デバイスが DHCP サーバに IP アドレス、サブネットマスク、ゲートウェイ IP アドレス、および DNS サーバを割り当てるように指示し、ドメイン名（オプション 15）、ホスト名（オプション 12）、およびクライアント完全修飾ドメイン名（FQDN）も要求します。</p> <p>無効になっている場合は、これらのパラメータを手動で設定する必要があります。</p>
IP Address	<p>デバイスの IP アドレス。DHCP が無効になっている場合は、このフィールドを有効な IP アドレスに設定する必要があります。DHCP が有効になっている場合は、このフィールドを編集することができません。</p>
Subnet Mask	<p>デバイスのサブネットマスク。DHCP が無効になっている場合は、このフィールドを有効なサブネットマスクに設定する必要があります。DHCP が有効になっている場合は、このフィールドを編集することができません。</p> <p>警告：不正な IP アドレス/サブネットマスクの組み合わせ（無効なマスクなど）を設定すると、デバイスにアクセスできなくなる可能性があります。サブネットマスクの設定は慎重に行ってください。</p>
Gateway	<p>デバイスのゲートウェイ IP アドレス。DHCP が無効になっている場合は、このフィールドが必須です。DHCP が有効になっている場合は、このフィールドを編集することができません。</p>
Primary DNS Server	<p>デバイスのプライマリ DNS IP アドレス。このフィールドは省略可能です。コネクションマネージャの使用中に DNS サーバの IP アドレスが設定された場合は、コネクションマネージャアドレスを IP アドレスの代わりに FQDN として設定することができます。</p>
Secondary DNS Server	<p>デバイスのセカンダリ DNS IP アドレス。このフィールドは省略可能です。コネクションマネージャの使用中に DNS サーバの IP アドレスが設定された場合は、コネクションマネージャアドレスを IP アドレスの代わりに FQDN として設定することができます。</p>
Domain Name	<p>ホストまたはクライアントのドメイン名（"domain.local"など）。このフィールドは省略可能です。</p>
FQDN	<p>ホストまたはクライアントの完全修飾ドメイン名。デフォルトは pcoip-host-<MAC>または pcoip-portal-<MAC>です。ここで、<MAC>はホストまたはクライアントの MAC アドレスです。使用された場合はドメイン名が付加されます（pcoip-host-<MAC>.domain.local など）。このページのこのフィールドは読み取り専用です。</p> <p>注意：FQDN 機能を使用するには、DHCP オプション 81 を使用した</p>

パラメータ	説明
	DNS サーバを用意して正しく設定する必要があります。
Ethernet Mode	<p>次のようにホストまたはクライアントのイーサネットモードを設定することができます。</p> <ul style="list-style-type: none"> • Auto • 100 Mbps Full-Duplex • 10 Mbps Full-Duplex <p>10 Mbps Full Duplex または 100 Mbps Full-Duplex を選択してから Apply をクリックすると、次の警告メッセージが表示されます。</p> <p>「Warning : When Auto-Negotiation is disabled on the PCoIP device, it must also be disabled on the switch. Additionally, the PCoIP device and switch must be configured to use the same speed and duplex parameters. Different parameters may result in a loss of network connectivity. Are you sure you want to continue?」</p> <p>パラメータを変更する場合は OK をクリックします。</p> <p>注意：他のネットワーク機器（スイッチなど）も 10 Mbps 全二重 または 100 Mbps 全二重 で動作するように設定されている場合は、必ず、イーサネットモードを Auto に設定し、10 Mbps Full-Duplex または 100 Mbps Full-Duplex 以外を使用しないようにする必要があります。イーサネットモードの設定が不適切な場合は、ネットワーク動作が PCoIP プロトコルでサポートされていない半二重になる可能性があります。セッションの品質が極端に低下して、最終的に停止します。</p>

5.3 ラベル設定

5.3.1 AWI : ラベル設定

Label ページでは、デバイスに名前を割り当てることができます。このページは、ホストまたはクライアントの **Configuration > Label** メニューから表示することができます。

Label

Change the PCoIP device labels

PCoIP Device Name:

Note: When DHCP is enabled the PCoIP Device Name is sent to the DHCP server as the requested hostname.

PCoIP Device Description:

Generic Tag:

図 5-6 : AWI Label ページ

表 5-10 : AWI Label ページパラメータ

パラメータ	説明
PCoIP Device Name	<p>ホストまたはクライアントに論理名を付けることができます。デフォルトは pcoip-host-<MAC>または pcoip-portal-<MAC>です。ここで、<MAC>はデバイスの MAC アドレスです。</p> <p>このフィールドは、DHCP が有効になっており、システムが DNS サーバへのホスト名登録をサポートするように設定されている場合に、ホストまたはクライアントが DNS サーバに登録する名前です</p> <p>PCoIP Device Name がネットワーク上のエンドポイントごとに一意であり、以下の命名規則に従っていることを保証することが重要です。</p> <ul style="list-style-type: none"> 先頭と末尾の文字はアルファベット (A~Z または a~z) または数字 (0~9) にする必要があります。 残りの文字はアルファベット、数字、またはハイフンに必要があります。 長さは 63 文字以下にする必要があります。
PCoIP Device Description	<p>デバイスのエンドポイントの場所など、デバイスの説明またはその他の情報。</p> <p>注意：ファームウェアはこのフィールドを使用しません。これは管理者専用のフィールドです。</p>
Generic Tag	<p>デバイスに関する汎用タグ情報。</p> <p>注意：ファームウェアはこのフィールドを使用しません。これは管理者専用のフィールドです。</p>

5.3.2 OSD : ラベル設定

Label ページでは、デバイスに名前を割り当てることができます。このページは、**Options > Configuration > Label** メニューから表示することができます。

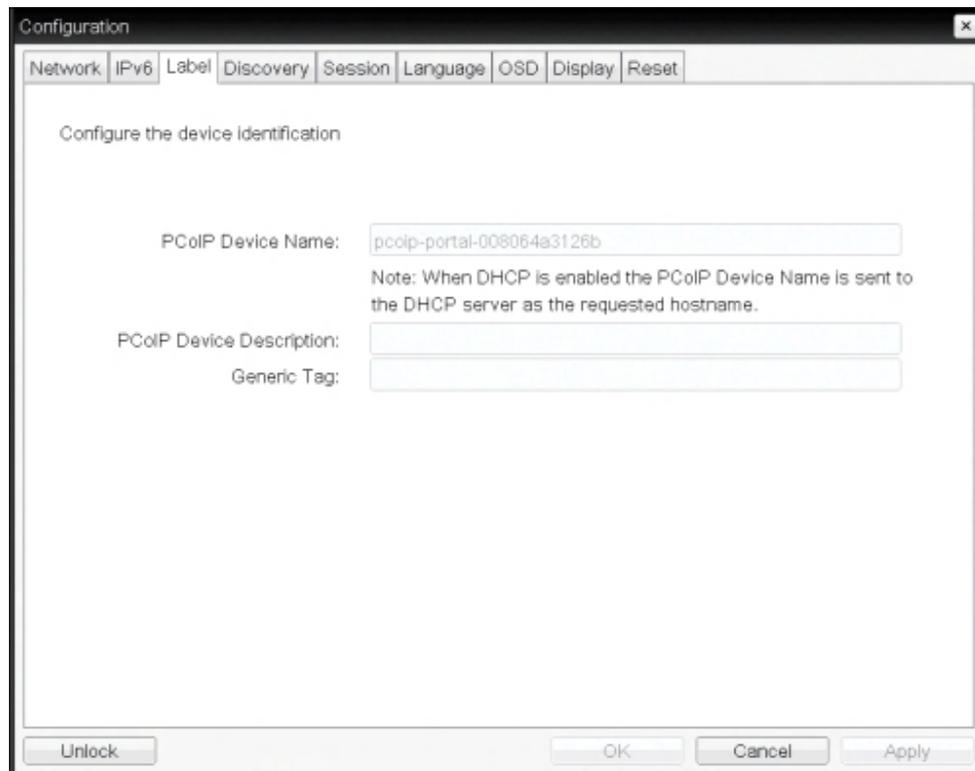


図 5-7 : OSD Label ページ

表 5-11 : OSD Label ページパラメータ

パラメータ	説明
PCoIP Device Name	<p>ホストまたはクライアントに論理名を付けることができます。デフォルトは <code>pcoip-host-<MAC></code> または <code>pcoip-portal-<MAC></code> です。ここで、<code><MAC></code> はデバイスの MAC アドレスです。</p> <p>このフィールドは、DHCP が有効になっており、システムが DNS サーバへのホスト名登録をサポートするように設定されている場合に、ホストまたはクライアントが DNS サーバに登録する名前です</p> <p>PCoIP Device Name がネットワーク上のエンドポイントごとに一意であり、以下の命名規則に従っていることを保証することが重要です。</p> <ul style="list-style-type: none"> 先頭と末尾の文字はアルファベット (A~Z または a~z) または数字 (0~9) にする必要があります。 残りの文字はアルファベット、数字、またはハイフンに必要があります。 長さは 63 文字以下にする必要があります。
PCoIP Device Description	<p>デバイスのエンドポイントの場所など、デバイスの説明またはその他の情報。</p> <p>注意：ファームウェアはこのフィールドを使用しません。これは管理</p>

パラメータ	説明
	者専用のフィールドです。
Generic Tag	デバイスに関する汎用タグ情報。 注意：ファームウェアはこのフィールドを使用しません。これは管理者専用のフィールドです。

5.4 デバイスディスカバリの設定

5.4.1 MC : ディスカバリ設定

このページの設定を使用すれば、ネットワーク上の場所に関する知識がなくても、SLP ディスカバリ、PCoIP MC DNS ベースのディスカバリプレフィックス、または DNS-SRV ディスカバリを使用して PCoIP システム内のホストとクライアントを動的に発見するようにプロファイルを構成することができます。ディスカバリメカニズムを使用すれば、複雑なシステムの設定工数と保守工数を大幅に減らすことができます。

注意：SLP ディスカバリメカニズムでは、すべての PCoIP デバイスと MC が同じネットワークサブネット上に存在する必要があります。SLP ディスカバリをサブネット全体で機能させるためには、サブネット間でマルチキャストトラフィックを転送するようにルータを設定する必要があります。ほとんどのデプロイメントではこれが不可能なため、DNS-SRV ディスカバリをお勧めします。

MC でプロパティを有効にするには、**Set in Profile** チェックボックスをオンにし、指示に従ってフィールドを設定します。このページでプロパティを更新したら、**Save** をクリックして変更を保存します。

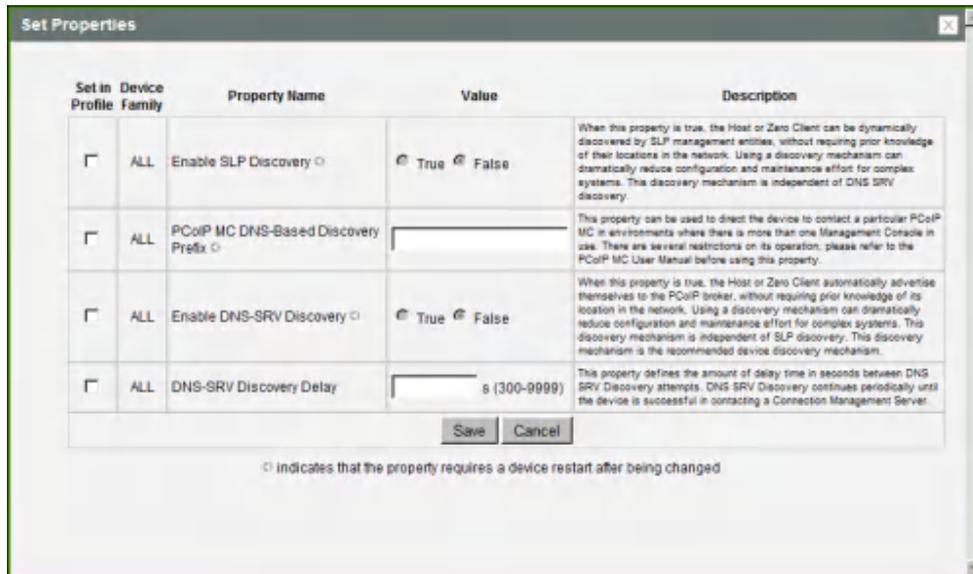


図 5-8 : MC ディスカバリ設定

表 5-12 : MC ディスカバリ設定パラメータ

パラメータ	説明
Enable SLP Discovery	有効になっている場合は、ホストとクライアントを、SLP 管理エンティティを通して動的に発見することができます。 注意：このプロパティを変更した場合はデバイスを再起動する必要があります。
PCoIP MC DNS-Based Discovery Prefix	このプロパティは、複数の管理コンソールが使用されている環境内の特定の PCoIP MC にデバイスから接触するように指示するために使用します。この動作にはいくつかの制約があります。このプロパティを使用する前に、『PCoIP Management Console User Manual』（TER0812002）を参照してください。 注意：このプロパティを変更した場合はデバイスを再起動する必要があります。
Enable DNS-SRV Discovery	有効になっている場合： <ul style="list-style-type: none"> ホストとクライアントが、ネットワーク上の場所に関する知識がなくても、自動的に、自らをコネクションブローカにアダプタイズします。 ホストまたはクライアントが DNS から DNS SRV レコードをダウンロードして使用しようとしています。 このディスカバリメカニズムの詳細については、『PCoIP Management Console User Manual』（TER0812002）を参照してください。 注意：このプロパティを変更した場合はデバイスを再起動する必要があります。

パラメータ	説明
DNS-SRV Discovery Delay	コネクションブローカと管理コンソールに対して DNS SRV ディスカバリを試みる時間間隔を秒単位で設定します。DNS SRV ディスカバリは、デバイスが接続管理サーバに正常に接触するまで定期的に繰り返されます。

5.4.2 AWI : ディスカバリ設定

このページの設定を使用すれば、ネットワーク上の場所に関する知識がなくても、管理エンティティを通して、PCoIP システム内のホストとクライアントを動的に発見することができます。ディスカバリメカニズムを使用すれば、複雑なシステムの設定工数と保守工数を大幅に減らすことができます。

このページは、ホストまたはクライアントの **Configuration > Discovery** メニューから表示することができます。

注意：SLP ディスカバリメカニズムでは、すべての PCoIP デバイスと MC が同じネットワークサブネット上に存在する必要があります。SLP ディスカバリをサブネット全体で機能させるためには、サブネット間でマルチキャストトラフィックを転送するようにルータを設定する必要があります。ほとんどのデプロイメントではこれが不可能なため、DNS-SRV ディスカバリをお勧めします。

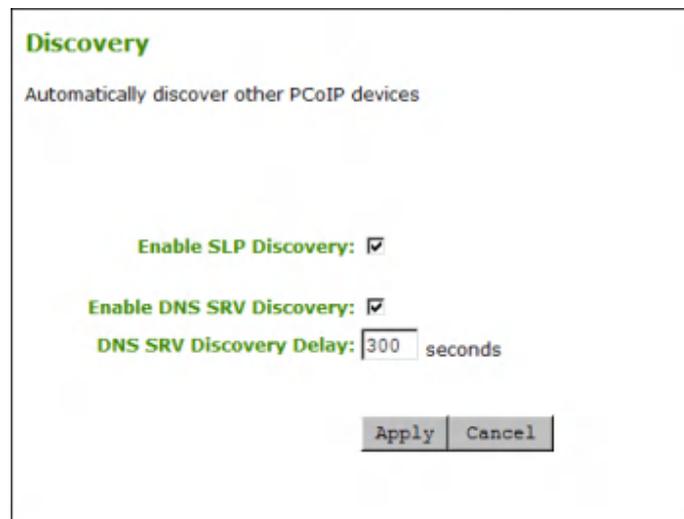


図 5-9 : AWI Discovery ページ

表 5-13 : AWI Discovery ページパラメータ

パラメータ	説明
Enable SLP Discovery	有効になっている場合は、ホストとクライアントを、SLP 管理エンティティを通して動的に発見することができます。

パラメータ	説明
Enable DNS-SRV Discovery	<p>有効になっている場合：</p> <ul style="list-style-type: none"> ホストとクライアントが、ネットワーク上の場所に関する知識がなくても、自動的に、自らをコネクシオンブローカにアダプタイズします。 ホストまたはクライアントが DNS から DNS SRV レコードをダウンロードして使用しようとしています。 <p>このディスカバリメカニズムの詳細については、『PCoIP Management Console User Manual』（TER0812002）を参照してください。</p> <p>注意：Enable DNS SRV Discovery オプションは、コネクシオンブローカのディスカバリを設定しますが、PCoIP 管理コンソールの DNS SRV 機能に影響を与えません。</p>
DNS-SRV Discovery Delay	<p>コネクシオンブローカと管理コンソールに対して DNS SRV ディスカバリを試みる時間間隔を秒単位で設定します。DNS SRV ディスカバリは、デバイスが接続管理サーバに正常に接触するまで定期的に繰り返されます。</p> <p>注意：Enable DNS SRV オプションは PCoIP 管理コンソールの DNS SRV 機能に影響を与えません。PCoIP 管理コンソールには DNS SRV Discovery Delay が使用されます。DNS SRV レコードがインストールされていない場合は、遅延を最大値の“9999”に設定することをお勧めします。これにより、ホストまたはクライアントによる PCoIP 管理コンソールへの接触の試みが最小限に抑えられます。</p>

5.4.3 OSD : ディスカバリ設定

このページの設定を使用すれば、ネットワーク上の場所に関する知識がなくても、サービスロケーションプロトコル（SLP）管理エンティティを通して、PCoIP システム内のホストとクライアントを動的に発見することができます。ディスカバリメカニズムを使用すれば、複雑なシステムの設定工数と保守工数を大幅に減らすことができます。

このページは、**Options > Configuration > Discovery** メニューから表示することができます。

注意：SLP ディスカバリメカニズムでは、すべての PCoIP デバイスと MC が同じネットワークサブネット上に存在する必要があります。SLP ディスカバリをサブネット全体で機能させるためには、サブネット間でマルチキャストトラフィックを転送するようにルータを設定する必要があります。ほとんどのデプロイメントではこれが不可能なため、DNS-SRV ディスカバリをお勧めします。これは、AWI [Discovery](#) ページまたは MC [Discovery Configuration](#) ページから設定することができます。

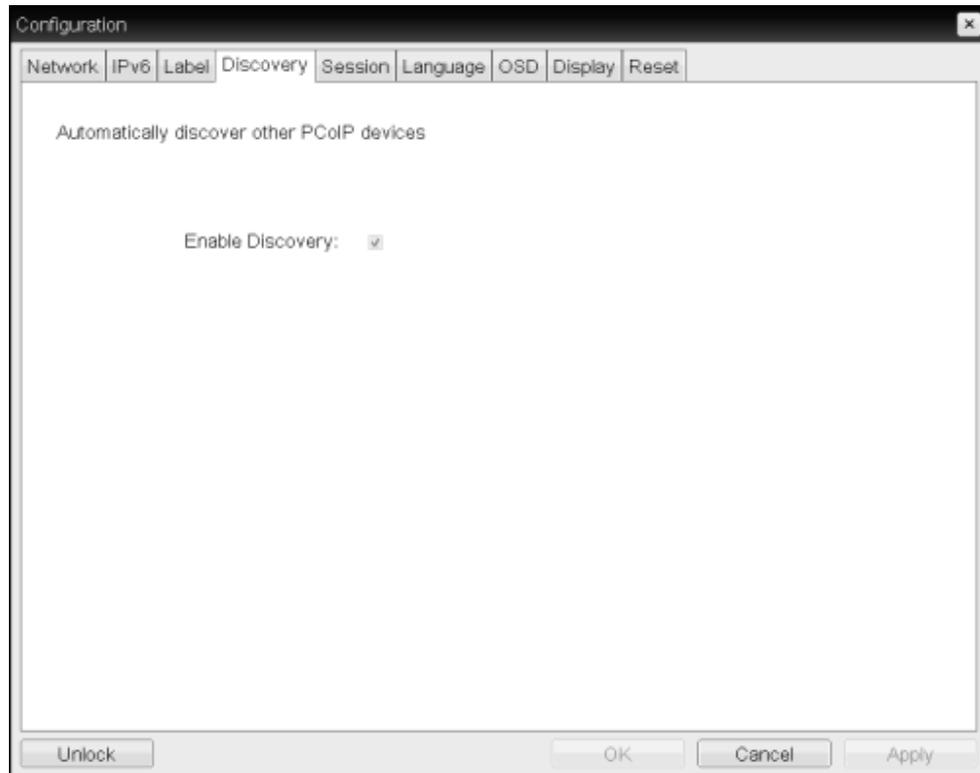


図 5-10 : OSD Discovery ページ

表 5-14 : OSD Discovery ページパラメータ

パラメータ	説明
Enable Discovery	有効になっている場合は、ホストを、SLP 管理エンティティを通して動的に発見することができます。

5.5 SNMP の設定

5.5.1 MC : SNMP 設定に関するヘルプ

管理コンソール用の SNMP 設定は、MC の [Network Configuration](#) ページに配置されています。

注意 : PCoIP SNMP エージェントの使用方法については、『Using SNMP with a PCoIP Device User Guide』 (TER0805002) を参照してください。

5.5.2 AWI : SNMP 設定

SNMP ページでは、ホストまたはクライアントの SNMP エージェントを有効または無効にすることができます。このページは、ホストまたはクライアントの **Configuration > SNMP** メニューから表示することができます。

注意：PCoIP SNMP エージェントの使用方法については、『Using SNMP with a PCoIP Device User Guide』（TER0805002）を参照してください。



図 5-11 : AWI SNMP ページ

表 5-15 : AWI SNMP ページパラメータ

パラメータ	説明
Enable SNMP	有効になっている場合は、デバイスが PCoIP SNMP エージェントから SNMP 要求に応答できるようにします。SNMP エージェントを無効にすると、SNMP 要求に応答することも、トラップを生成することもできなくなります。また、PCoIP SNMP MIB にアクセスすることもできなくなります。
Community Name	デバイスで使用される SNMP コミュニティ名を設定します。

5.6 セッションの設定

5.6.1 セッションの設定

MC、AWI、および OSD 上の **Session** ページでは、ホストまたはクライアントデバイスからピアデバイスへの接続方法やホストまたはクライアントデバイスのピアデバイスからの接続の受け入れ方法を設定することができます。使用可能な設定オプションは、選択されたセッション接続タイプによって異なります。

セッション接続タイプ

次の 3 つの主なセッション接続タイプがあります。

- [Direct to Host](#) (SLP ホストディスカバリを使用するためのオプション付き)
- [View Connection Server](#) (さまざまなオプション付き)
- [Connection Management Interface](#)

Direct to Host セッション

Direct to Host セッションは、ゼロクライアントと、PCoIP ホストカードが実装されたリモートワークステーション間の直接接続です。ホストの DNS 名または IP アド

レスを指定したり、クライアントを、サービスローケーションプロトコル (SLP) を通してホストを発見するように設定したりすることができます。セッションが失われたときに自動的にホストに再接続するようにクライアントを設定することもできます。

表 5-16 : 直接セッション接続

管理ツール	デバイス	セッション接続オプション
MC	すべてのデバイスファミリー	Direct to Host Direct to Host + SLP ホストディスカバリ
AWI	ホスト	Direct from Client
	クライアント	Direct to Host Direct to Host + SLP ホストディスカバリ
OSD	クライアント	Direct to Host Direct to Host + SLP ホストディスカバリ

VMware View 仮想デスクトップ接続

VMware View セッションは、VMware View Connection Server とコネクションマネージャ ([コネクションブローカ](#)とも呼ばれる) を使用したゼロクライアントと VMware View 仮想デスクトップ間の接続です。VMware View セッションは、基本モード、自動ログオンモード、VMware View キオスクモード、および Imprivata OneSign モードで設定することができます。

表 5-17 : 直接セッション接続

管理ツール	デバイス	セッション接続オプション
MC	すべてのデバイスファミリー	View Connection Server View Connection Server + 自動ログオン View Connection Server + キオスク View Connection Server + Imprivata OneSign
AWI	クライアント	View Connection Server View Connection Server + 自動ログオン View Connection Server + キオスク View Connection Server + Imprivata OneSign
OSD	クライアント	View Connection Server View Connection Server + 自動ログオン

管理ツール	デバイス	セッション接続オプション
		View Connection Server + キオスク View Connection Server + Imprivata OneSign

Connection Management Interface セッション

Connection Management Interface は、外部のコネクションマネージャを [コネクションブローカ](#) として設定するために使用します。

表 5-18 : 直接セッション接続

管理ツール	デバイス	セッション接続オプション
MC	すべてのデバイスファミリー	Connection Management Interface
AWI	ホスト	Connection Management Interface
	クライアント	Connection Management Interface
OSD	クライアント	Connection Management Interface

5.6.2 MC : Direct to Host セッション設定

クライアントを直接ホストに接続するようにプロファイルを設定するには、MC で **Direct to Host** セッション接続タイプを選択します。

MC でプロパティを有効にするには、**Set in Profile** チェックボックスをオンにし、指示に従ってフィールドを設定します。このページでプロパティを更新したら、**Save** をクリックして変更を保存します。

この選択を変更した場合はデバイスを再起動する必要があります。

注意：特定のホストとクライアントのリンク方法については、『PCoIP Management Console User Manual』（TER0812002）を参照してください。ピアリングプロパティを使用して特定のホストを設定する（特定の MAC アドレスではなく任意のピアを受け入れるするためなど）には、AWI の [Direct from Client](#) セッション設定を使用します。

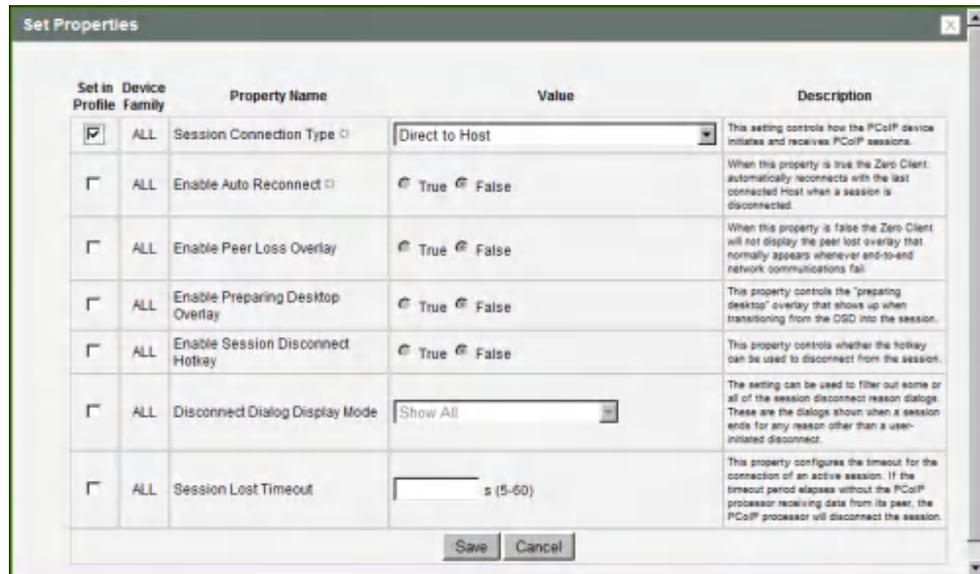


図 5-12 : MC セッション接続タイプ – Direct to Host

表 5-19 : MC セッション設定パラメータ

パラメータ	説明
Enable Auto Reconnect	有効になっている場合は、セッションが失われたときに、クライアントが自動的に最後に接続していたホストに再接続します。 注意：このプロパティを変更した場合はデバイスを再起動する必要があります。
Enable Peer Loss Overlay	有効になっている場合は、ネットワーク接続の消失が検出されたときに、“Network Connection Lost”オーバーレイがディスプレイ上に表示されます。このオーバーレイは VMware View などの仮想デスクトップの場合にも表示されます。通常のハイパーバイザスケジューリングの遅延によってもこのメッセージが誤ってトリガーされる場合があります。 注意：このオプションはゼロクライアントに対してしか使用することができません。ピア消失通知が必要なデスクトップアプリケーションは、OSD、AWI、または MC を介してこの機能を再有効化する必要があります。
Enable Preparing Desktop Overlay	有効になっている場合は、ユーザがログインしたときに、“Preparing Desktop”オーバーレイがディスプレイ上に表示されます。 注意：このオーバーレイは、デスクトップの表示に数秒以上かかっている場合でもログインが進行中であることを保証します。
Disconnect Dialog Display Mode	このフィールドを使用すれば、セッションが切断されたときに表示されるメッセージのタイプを制御することができます。次の 3 つのカテゴリに分かれています。

パラメータ	説明
	<p>情報：セッションに影響を与えるユーザまたは管理者によるアクション：</p> <ul style="list-style-type: none"> • 別の場所からログインしたか、ホストがシャットダウンまたは再起動されたために切断されました。 • 管理者が切断を実行したために切断されました。 • 別の場所からログインしたために切断されました。 • ワークステーションを切断したために切断されました。 <p>警告：セッションに影響を与えるシステムによる予想されるアクション：</p> <ul style="list-style-type: none"> • セッションがタイムアウトしたために切断されました。 <p>エラー：セッションの失敗を引き起こす予期せぬシステムによるアクション：</p> <ul style="list-style-type: none"> • 切断されました。 • 接続できません (0x1001)。IT 管理者に連絡してください。 • 接続できません (0x1002)。IT 管理者に連絡してください。 • セッションがリモートで閉じられました。 • セッションがリモートで閉じられました (原因不明)。 • 設定エラーが原因で切断されました (0x100)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x201)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x300)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x301)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x302)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x303)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x305)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x400)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x401)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x402)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x403)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x404)。IT 管理者に支援を要請してください。 <p>以下の表示を選択することができます。</p> <p>1. Show All messages – このオプションは、情報メッセージ、警告メッセージ、およびエラーメッセージを含むすべての切断メッセ</p>

パラメータ	説明
	<p>ージを表示します。</p> <p>2. Show Error and Warnings Only – このオプションは情報メッセージを表示せず、エラーメッセージと警告メッセージのみを表示します。</p> <p>3. Show Error Only – このオプションは情報メッセージと警告メッセージを表示せず、エラーメッセージのみを表示します。</p> <p>4. Show None – どの切断メッセージも表示しません。</p>
Session Lost Timeout	<p>アクティブセッションの接続に関するタイムアウト（秒単位）を入力します。このフィールドの有効タイムアウト範囲は 5～60 秒です。このタイムアウト期間が満了になるとセッションが切断されます。</p>

5.6.3 MC : Direct to Host Session + SLP ホストディスカバリ設定

クライアントを直接ホストに接続するようにプロファイルを設定して、サービスローケーションプロトコル（SLP）を通してホストを動的に発見するようにクライアントを設定する場合は、MC で **Direct to Host + SLP ホストディスカバリセッション** 接続タイプを選択します。

MC でプロパティを有効にするには、**Set in Profile** チェックボックスをオンにし、指示に従ってフィールドを設定します。このページでプロパティを更新したら、**Save** をクリックして変更を保存します。

この選択を変更した場合はデバイスを再起動する必要があります。

注意：特定のホストとクライアントのリンク方法については、『[PCoIP Management Console User Manual](#)』（TER0812002）を参照してください。ピアリングプロパティを使用して特定のホストを設定する（特定の MAC アドレスではなく任意のピアを受け入れるためなど）には、AWI の [Direct from Client](#) セッション設定を使用します。

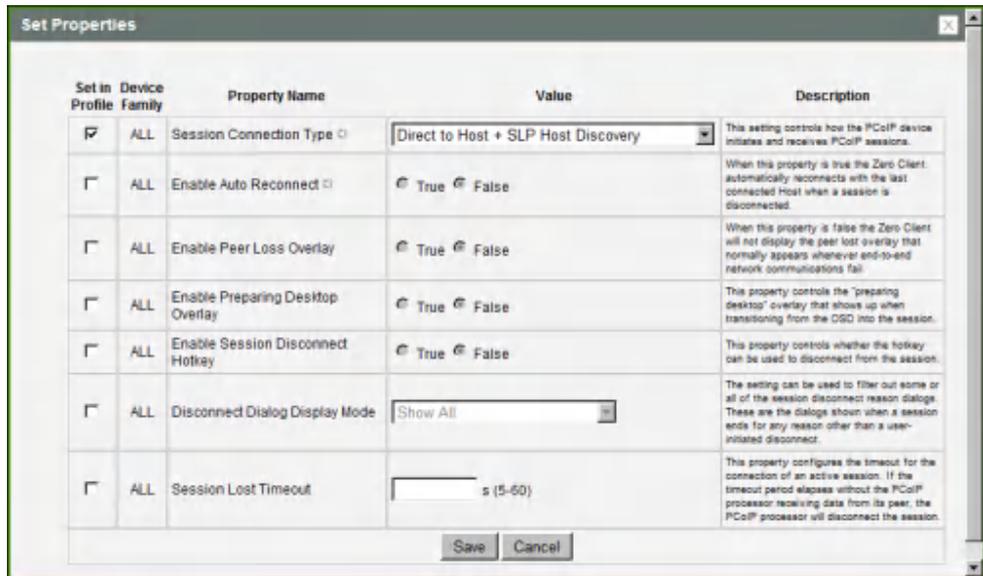


図 5-13 : MC セッション接続タイプ – Direct to Host + SLP ホストディスカバリ

表 5-20 : MC セッション設定パラメータ

パラメータ	説明
Enable Auto Reconnect	有効になっている場合は、セッションが失われたときに、クライアントが自動的に最後に接続していたホストに再接続します。 注意：このプロパティを変更した場合はデバイスを再起動する必要があります。
Enable Peer Loss Overlay	有効になっている場合は、ネットワーク接続の消失が検出されたときに、“Network Connection Lost”オーバーレイがディスプレイ上に表示されます。このオーバーレイは VMware View などの仮想デスクトップの場合にも表示されます。通常のハイパーバイザスケジューリングの遅延によってもこのメッセージが誤ってトリガーされる場合があります。 注意：このオプションはゼロクライアントに対してしか使用することができません。ピア消失通知が必要なデスクトップアプリケーションは、OSD、AWI、または MC を介してこの機能を再有効化する必要があります。
Enable Preparing Desktop Overlay	有効になっている場合は、ユーザがログインしたときに、“Preparing Desktop”オーバーレイがディスプレイ上に表示されます。 注意：このオーバーレイは、デスクトップの表示に数秒以上かかっている場合でもログインが進行中であることを保証します。
Disconnect Dialog Display Mode	このフィールドを使用すれば、セッションが切断されたときに表示されるメッセージのタイプを制御することができます。次の 3 つのカテゴリに分かれています。

パラメータ	説明
	<p>情報：セッションに影響を与えるユーザまたは管理者によるアクション：</p> <ul style="list-style-type: none"> • 別の場所からログインしたか、ホストがシャットダウンまたは再起動されたために切断されました。 • 管理者が切断を実行したために切断されました。 • 別の場所からログインしたために切断されました。 • ワークステーションを切断したために切断されました。 <p>警告：セッションに影響を与えるシステムによる予想されるアクション：</p> <ul style="list-style-type: none"> • セッションがタイムアウトしたために切断されました。 <p>エラー：セッションの失敗を引き起こす予期せぬシステムによるアクション：</p> <ul style="list-style-type: none"> • 切断されました。 • 接続できません (0x1001)。IT 管理者に連絡してください。 • 接続できません (0x1002)。IT 管理者に連絡してください。 • セッションがリモートで閉じられました。 • セッションがリモートで閉じられました (原因不明)。 • 設定エラーが原因で切断されました (0x100)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x201)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x300)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x301)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x302)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x303)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x305)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x400)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x401)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x402)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x403)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x404)。IT 管理者に支援を要請してください。 <p>以下の表示を選択することができます。</p> <ol style="list-style-type: none"> 1. Show All messages – このオプションは、情報メッセージ、警告メッセージ、およびエラーメッセージを含むすべての切断メッセ

パラメータ	説明
	<p>ージを表示します。</p> <p>2. Show Error and Warnings Only – このオプションは情報メッセージを表示せず、エラーメッセージと警告メッセージのみを表示します。</p> <p>3. Show Error Only – このオプションは情報メッセージと警告メッセージを表示せず、エラーメッセージのみを表示します。</p> <p>4. Show None – どの切断メッセージも表示しません。</p>
Session Lost Timeout	アクティブセッションの接続に関するタイムアウト（秒単位）を入力します。このフィールドの有効タイムアウト範囲は5~60秒です。このタイムアウト期間が満了になるとセッションが切断されます。

5.6.4 MC : View Connection Server セッション設定

VMware View Connection Server を使用してクライアントを仮想デスクトップに接続するようにプロファイルを設定する場合は、MC で **View Connection Server** セッション接続タイプを選択します。

MC でプロパティを有効にするには、**Set in Profile** チェックボックスをオンにし、指示に従ってフィールドを設定します。このページでプロパティを更新したら、**Save** をクリックして変更を保存します。

この選択を変更した場合はデバイスを再起動する必要があります。

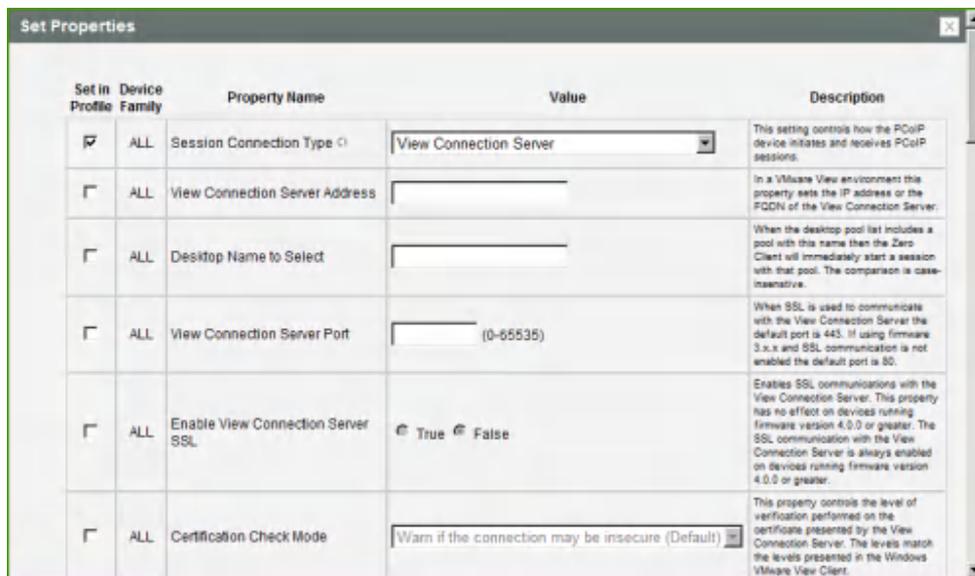


図 5-14 : MC セッション接続タイプ – View Connection Server

表 5-21 : MC セッション設定パラメータ

パラメータ	説明

パラメータ	説明
View Connection Server Address	View Connection Server の IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。
Desktop Name to Select	セッションを開始するときにクライアントが使用するプール/デスクトップ名を入力します。 注意：この設定は省略可能です。
View Connection Server Port	View Connection Server との通信に SSL が使用されている場合のデフォルトポートは 443 です。SSL 通信が無効になっている場合のデフォルトポートは 80 です。 ネットワークがセキュア接続用として非標準ポートを使用するようにセットアップされている場合は、ポート番号を入力します。
Enable View Connection Server SSL	有効になっている場合は、View Connection Server との SSL 通信が可能になります。 注意：このプロパティは、View Connection Server との SSL 通信が常に有効になっているファームウェア 4.0.0 以降を実行しているデバイスには影響を与えません。
Certification Check Mode	クライアントが View Connection Server とのセキュア接続を確認できない場合の動作を選択します。 <ul style="list-style-type: none"> • Warn if the connection may be insecure (Default) : 未署名のまたは期限切れの証明書を受信した場合、または、証明書が自己署名されておらず、ゼロクライアントのトラストストアが空の場合に警告を表示するようにクライアントを設定します (このオプションはデフォルトで選択されています)。 • Reject the unverifiable connection (Secure) : 信頼できる有効な証明書がインストールされていない場合に接続を拒否するようにクライアントを設定します。 • Allow the unverifiable connection (Not Secure) : すべての接続を許可するようにクライアントを設定します。
Certification Check Lockout Mode	ユーザが OSD から VCS Certificate Check Mode 設定を変更できないようにする場合は、このプロパティを Locked に設定します。
Clear Trusted Connection Server Cache	有効になっている場合は、信頼できる View Connection Server のキャッシュがクリアされます。
Enable View Connection Server Auto Connect	有効になっている場合は、クライアントが、電源がオンになっているときはいつでも、または、仮想デスクトップとのセッションが終了したときに、自動的に、選択された View Connection Server に接続します。

パラメータ	説明
Connection Server Cache Mode	<p>このフィールドは、ユーザが有効なサーバアドレスを入力したときに View Connection Server を OSD Connect ページの Server ドロップダウンメニューに動的に追加するかどうか、または、ユーザが選択するための読み取り専用リストに View Connection Server を表示するかどうかを決定します。</p> <ul style="list-style-type: none"> • Last servers used : ユーザが入力したキャッシュサーバのリストを OSD Connect ページの Server ドロップダウンメニューに表示したい場合にこのオプションを選択します。 • Read-only : ユーザに読み取り専用リストから View Connection Server を選択させたい場合にこのオプションを選択します。
Connection Server Cache Entry (1 to 25)	<p>ユーザの OSD Connect ページ内のキャッシュに表示する、必要な数のフィールド (最大 25) を有効にして、それぞれに対して、ユーザの接続を許可する View Connection Server の IP アドレスまたは FQDN を入力します。</p> <ul style="list-style-type: none"> • Connection Server Cache Mode フィールドで Last servers used が選択されている場合は、ユーザが有効なサーバ IP アドレスまたは FQDN を入力するたびに新しい View Connection Server が Server ドロップダウンメニューに追加されます。 • Read-only が選択されている場合は、ユーザは Server ドロップダウンメニュー内の読み取り専用リストからしかサーバを選択することができません。
Self Help Link Mode	<p>有効になっている場合は、VMware View ユーザ認証画面上でセルフヘルプリンクが有効になります。</p>
Auto Launch If Only One Desktop	<p>有効になっている場合は、ユーザ資格情報の入力後に、自動的に、ユーザが仮想デスクトップに接続されます。</p>
Enable Login Username Caching	<p>有効になっている場合は、ユーザ名テキストボックスに、自動的に、最後に入力されたユーザ名が設定されます。</p>
Use OSD Logo for View Banner	<p>有効になっている場合は、ログイン中に、VMware View バナーの代わりに、PCoIP ゼロクライアント OSD ロゴが表示されます。OSD ロゴは OSD Logo Upload ページでアップロードすることができます。</p>
Prefer GSC-IS Over PIV Endpoint	<p>選択されている場合は、スマートカードで CAC (GSC-IS) や PIV エンドポイントなどの複数のインターフェースがサポートされていれば、GSC-IS インターフェースが使用されます。スマートカードで CAC と PIV エンドポイントのどちらかなどの 1 つのインターフェースしかサポートされていない場合は、この設定に関係なく、CAC または PIV エンドポイントインターフェースのみが使用されます。これは、PCoIP セッション以外で実行されるスマートカードアクセスにのみ影響を与えます。</p>
Enable Peer Loss	<p>有効になっている場合は、ネットワーク接続の消失が検出されたとき</p>

パラメータ	説明
Overlay	<p>に、“Network Connection Lost”オーバーレイがディスプレイ上に表示されます。このオーバーレイは VMware View などの仮想デスクトップの場合にも表示されます。通常のハイパーバイザスケジューリングの遅延によってもこのメッセージが誤ってトリガーされる場合があります。</p> <p>注意：このオプションはゼロクライアントに対してしか使用することができません。ピア消失通知が必要なデスクトップアプリケーションは、OSD、AWI、または MC を介してこの機能を再有効化する必要があります。</p>
Enable Preparing Desktop Overlay	<p>有効になっている場合は、ユーザがログインしたときに、“Preparing Desktop”オーバーレイがディスプレイ上に表示されます。</p> <p>注意：このオーバーレイは、デスクトップの表示に数秒以上かかっている場合でもログインが進行中であることを保証します。</p>
Disconnect Dialog Display Mode	<p>このフィールドを使用すれば、セッションが切断されたときに表示されるメッセージのタイプを制御することができます。次の 3 つのカテゴリに分かれています。</p> <p>情報：セッションに影響を与えるユーザまたは管理者によるアクション：</p> <ul style="list-style-type: none"> • 別の場所からログインしたか、ホストがシャットダウンまたは再起動されたために切断されました。 • 管理者が切断を実行したために切断されました。 • 別の場所からログインしたために切断されました。 • ワークステーションを切断したために切断されました。 <p>警告：セッションに影響を与えるシステムによる予想されるアクション：</p> <ul style="list-style-type: none"> • セッションがタイムアウトしたために切断されました。 <p>エラー：セッションの失敗を引き起こす予期せぬシステムによるアクション：</p> <ul style="list-style-type: none"> • 切断されました。 • 接続できません (0x1001)。IT 管理者に連絡してください。 • 接続できません (0x1002)。IT 管理者に連絡してください。 • セッションがリモートで閉じられました。 • セッションがリモートで閉じられました (原因不明)。 • 設定エラーが原因で切断されました (0x100)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x201)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x300)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x301)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x302)。IT 管理者に支援

パラメータ	説明
	<p>を要請してください。</p> <ul style="list-style-type: none"> • 設定エラーが原因で切断されました (0x303)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x305)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x400)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x401)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x402)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x403)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x404)。IT 管理者に支援を要請してください。 <p>以下の表示を選択することができます。</p> <ol style="list-style-type: none"> 1. Show All messages – このオプションは、情報メッセージ、警告メッセージ、およびエラーメッセージを含むすべての切断メッセージを表示します。 2. Show Error and Warnings Only – このオプションは情報メッセージを表示せず、エラーメッセージと警告メッセージのみを表示します。 3. Show Error Only – このオプションは情報メッセージと警告メッセージを表示せず、エラーメッセージのみを表示します。 4. Show None – どの切断メッセージも表示しません。
Session Lost Timeout	<p>アクティブセッションの接続に関するタイムアウト (秒単位) を入力します。このフィールドの有効タイムアウト範囲は 5~60 秒です。このタイムアウト期間が満了になるとセッションが切断されます。</p>

5.6.5 MC : View Connection Server + 自動ログオンセッション設定

クライアントが VMware View Connection Server 経由で仮想デスクトップに接続するときに自動的にユーザのログイン詳細を入力するようにプロファイルを設定する場合は、MC で **View Connection Server + 自動ログオンセッション** 接続タイプを選択します。

MC でプロパティを有効にするには、**Set in Profile** チェックボックスをオンにし、指示に従ってフィールドを設定します。このページでプロパティを更新したら、**Save** をクリックして変更を保存します。

この選択を変更した場合はデバイスを再起動する必要があります。

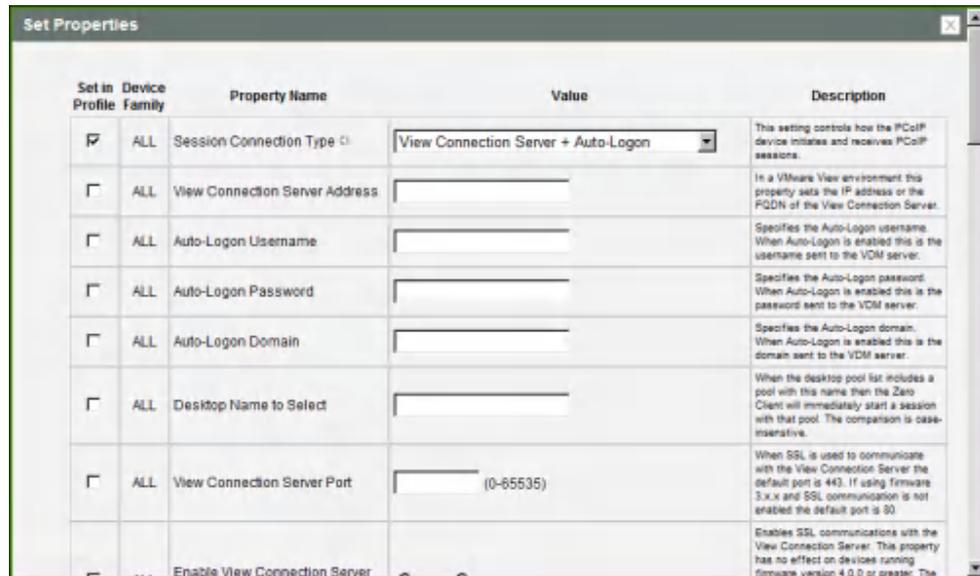


図 5-15 : MC セッション接続タイプ – View Connection Server + 自動ログオン

表 5-22 : MC セッション設定パラメータ

パラメータ	説明
View Connection Server Address	View Connection Server の IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。
Auto-Logon Username	指定した View Connection Server に送信するユーザ名を入力します。
Auto-Logon Password	指定した View Connection Server に送信するパスワードを入力します。
Auto-Logon Domain	指定した View Connection Server に送信するドメインを入力します。
Desktop Name to Select	セッションを開始するときにクライアントが使用するプール/デスクトップ名を入力します。 注意：この設定は省略可能です。
View Connection Server Port	View Connection Server との通信に SSL が使用されている場合のデフォルトポートは 443 です。SSL 通信が無効になっている場合のデフォルトポートは 80 です。 ネットワークがセキュア接続用として非標準ポートを使用するようにセットアップされている場合は、ポート番号を入力します。
Enable View Connection	有効になっている場合は、View Connection Server との SSL 通信が

パラメータ	説明
Server SSL	可能になります。 注意：このプロパティは、View Connection Server との SSL 通信が常に有効になっているファームウェア 4.0.0 以降を実行しているデバイスには影響を与えません。
Certification Check Mode	クライアントが View Connection Server とのセキュア接続を確認できない場合の動作を選択します。 <ul style="list-style-type: none"> • Warn if the connection may be insecure (Default) : 未署名のまたは期限切れの証明書を受信した場合、または、証明書が自己署名されておらず、ゼロクライアントのトラストストアが空の場合に警告を表示するようにクライアントを設定します（このオプションはデフォルトで選択されています）。 • Reject the unverifiable connection (Secure) : 信頼できる有効な証明書がインストールされていない場合に接続を拒否するようにクライアントを設定します。 • Allow the unverifiable connection (Not Secure) : すべての接続を許可するようにクライアントを設定します。
Certification Check Lockout Mode	ユーザが OSD から VCS Certificate Check Mode 設定を変更できないようにする場合は、このプロパティを Locked に設定します。
Clear Trusted Connection Server Cache	有効になっている場合は、信頼できる View Connection Server のキャッシュがクリアされます。
Enable View Connection Server Auto Connect	有効になっている場合は、クライアントが、電源がオンになっているときはいつでも、または、仮想デスクトップとのセッションが終了したときに、自動的に、選択された View Connection Server に接続します。
Connection Server Cache Mode	このフィールドは、ユーザが有効なサーバアドレスを入力したときに View Connection Server を OSD Connect ページの Server ドロップダウンメニューに動的に追加するかどうか、または、ユーザが選択するための読み取り専用リストに View Connection Server を表示するかどうかを決定します。 <ul style="list-style-type: none"> • Last servers used : ユーザが入力したキャッシュサーバのリストを OSD Connect ページの Server ドロップダウンメニューに表示したい場合にこのオプションを選択します。 • Read-only : ユーザに読み取り専用リストから View Connection Server を選択させたい場合にこのオプションを選択します。
Connection Server Cache Entry (1 to 25)	ユーザの OSD Connect ページ内のキャッシュに表示する、必要な数のフィールド（最大 25）を有効にして、それぞれに対して、ユーザの接続を許可する View Connection Server の IP アドレスまたは FQDN を入力します。 <ul style="list-style-type: none"> • Connection Server Cache Mode フィールドで Last servers

パラメータ	説明
	<p>used が選択されている場合は、ユーザが有効なサーバ IP アドレスまたは FQDN を入力するたびに新しい View Connection Server が Server ドロップダウンメニューに追加されます。</p> <ul style="list-style-type: none"> • Read-only が選択されている場合は、ユーザは Server ドロップダウンメニュー内の読み取り専用リストからしかサーバを選択することができません。
Auto Launch If Only One Desktop	有効になっている場合は、ユーザ資格情報の入力後に、自動的に、ユーザが仮想デスクトップに接続されます。
Use OSD Logo for View Banner	有効になっている場合は、ログイン中に、VMware View バナーの代わりに、PCoIP ゼロクライアント OSD ロゴが表示されます。OSD ロゴは OSD Logo Upload ページでアップロードすることができます。
Enable Peer Loss Overlay	<p>有効になっている場合は、ネットワーク接続の消失が検出されたときに、“Network Connection Lost”オーバーレイがディスプレイ上に表示されます。このオーバーレイは VMware View などの仮想デスクトップの場合にも表示されます。通常のハイパーバイザスケジューリングの遅延によってもこのメッセージが誤ってトリガーされる場合があります。</p> <p>注意：このオプションはゼロクライアントに対してしか使用することができません。ピア消失通知が必要なデスクトップアプリケーションは、OSD、AWI、または MC を介してこの機能を再有効化する必要があります。</p>
Enable Preparing Desktop Overlay	<p>有効になっている場合は、ユーザがログインしたときに、“Preparing Desktop”オーバーレイがディスプレイ上に表示されます。</p> <p>注意：このオーバーレイは、デスクトップの表示に数秒以上かかっている場合でもログインが進行中であることを保証します。</p>
Disconnect Dialog Display Mode	<p>このフィールドを使用すれば、セッションが切断されたときに表示されるメッセージのタイプを制御することができます。次の 3 つのカテゴリに分かれています。</p> <p>情報：セッションに影響を与えるユーザまたは管理者によるアクション：</p> <ul style="list-style-type: none"> • 別の場所からログインしたか、ホストがシャットダウンまたは再起動されたために切断されました。 • 管理者が切断を実行したために切断されました。 • 別の場所からログインしたために切断されました。 • ワークステーションを切断したために切断されました。 <p>警告：セッションに影響を与えるシステムによる予想されるアクション：</p> <ul style="list-style-type: none"> • セッションがタイムアウトしたために切断されました。 <p>エラー：セッションの失敗を引き起こす予期せぬシステムによるアク</p>

パラメータ	説明
	<p>セッション：</p> <ul style="list-style-type: none"> • 切断されました。 • 接続できません (0x1001)。IT 管理者に連絡してください。 • 接続できません (0x1002)。IT 管理者に連絡してください。 • セッションがリモートで閉じられました。 • セッションがリモートで閉じられました (原因不明)。 • 設定エラーが原因で切断されました (0x100)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x201)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x300)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x301)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x302)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x303)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x305)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x400)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x401)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x402)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x403)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x404)。IT 管理者に支援を要請してください。 <p>以下の表示を選択することができます。</p> <ol style="list-style-type: none"> 1. Show All messages – このオプションは、情報メッセージ、警告メッセージ、およびエラーメッセージを含むすべての切断メッセージを表示します。 2. Show Error and Warnings Only – このオプションは情報メッセージを表示せず、エラーメッセージと警告メッセージのみを表示します。 3. Show Error Only – このオプションは情報メッセージと警告メッセージを表示せず、エラーメッセージのみを表示します。 4. Show None – どの切断メッセージも表示しません。
Session Lost Timeout	<p>アクティブセッションの接続に関するタイムアウト (秒単位) を入力します。このフィールドの有効タイムアウト範囲は 5~60 秒です。このタイムアウト期間が満了になるとセッションが切断されます。</p>

5.6.6 MC : View Connection Server + キオスクセッション設定

クライアントが VMware View Connection Server 経由で仮想デスクトップに接続するときにキオスクモードを使用するようにプロファイルを設定する場合は、MC で **View Connection Server + キオスクセッション** 接続タイプを選択します。

MC でプロパティを有効にするには、**Set in Profile** チェックボックスをオンにし、指示に従ってフィールドを設定します。このページでプロパティを更新したら、**Save** をクリックして変更を保存します。

この選択を変更した場合はデバイスを再起動する必要があります。

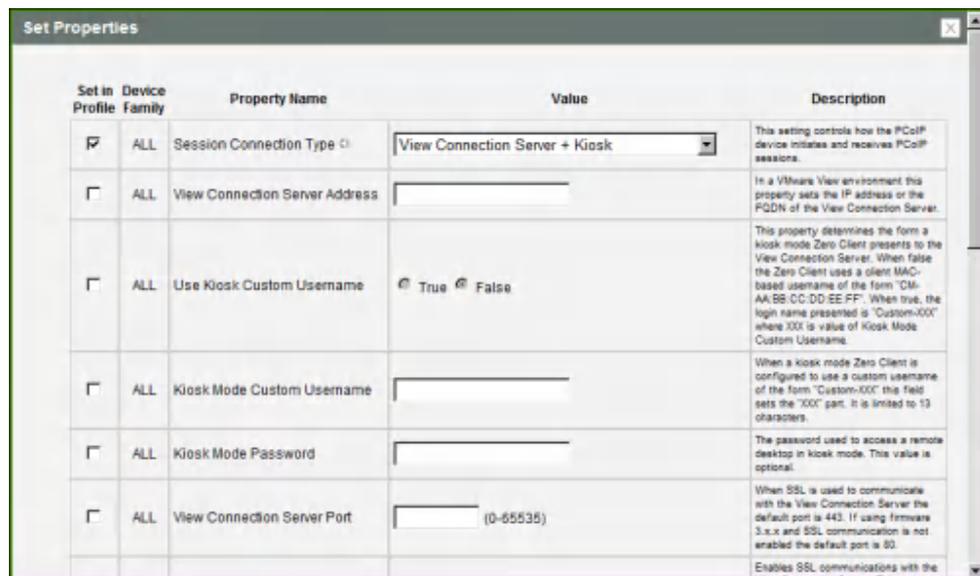


図 5-16 : MC セッション接続タイプ – View Connection Server + キオスク

表 5-23 : MC セッション設定パラメータ

パラメータ	説明
View Connection Server Address	View Connection Server の IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。
Use Kiosk Custom Username	有効になっている場合は、ログイン名が "Custom-<XXX>" として表示されます。ここで、"XXX" は Kiosk Mode Custom Username の値です。無効になっている場合は、クライアントが "CM-AA:BB:CC:DD:EE:FF" という形式の MAC ベースのユーザ名を使用します。
Kiosk Mode Custom Username	Use Kiosk Custom Username が "Custom-<XXX>" という形式のカスタムユーザ名を使用するように設定されている場合に、"XXX" コンポーネントの値を入力します。このフィールドは最大 13 文字に制限されています。

パラメータ	説明
Kiosk Mode Password	<p>キオスクモードで仮想デスクトップにアクセスするためのパスワードを入力します。</p> <p>注意：この設定は省略可能です。</p>
View Connection Server Port	<p>View Connection Server との通信に SSL が使用されている場合のデフォルトポートは 443 です。SSL 通信が無効になっている場合のデフォルトポートは 80 です。</p> <p>ネットワークがセキュア接続用として非標準ポートを使用するようにセットアップされている場合は、ポート番号を入力します。</p>
Enable View Connection Server SSL	<p>有効になっている場合は、View Connection Server との SSL 通信が可能になります。</p> <p>注意：このプロパティは、View Connection Server との SSL 通信が常に有効になっているファームウェア 4.0.0 以降を実行しているデバイスには影響を与えません。</p>
Certification Check Mode	<p>クライアントが View Connection Server とのセキュア接続を確認できない場合の動作を選択します。</p> <ul style="list-style-type: none"> • Warn if the connection may be insecure (Default) : 未署名のまたは期限切れの証明書を受信した場合、または、証明書が自己署名されておらず、ゼロクライアントのトラストストアが空の場合に警告を表示するようにクライアントを設定します（このオプションはデフォルトで選択されています）。 • Reject the unverifiable connection (Secure) : 信頼できる有効な証明書がインストールされていない場合に接続を拒否するようにクライアントを設定します。 • Allow the unverifiable connection (Not Secure) : すべての接続を許可するようにクライアントを設定します。
Certification Check Lockout Mode	<p>ユーザが OSD から VCS Certificate Check Mode 設定を変更できないようにする場合は、このプロパティを Locked に設定します。</p>
Clear Trusted Connection Server Cache	<p>有効になっている場合は、信頼できる View Connection Server のキャッシュがクリアされます。</p>
Use OSD Logo for View Banner	<p>有効になっている場合は、ログイン中に、VMware View バナーの代わりに、PCoIP ゼロクライアント OSD ロゴが表示されます。OSD ロゴは OSD Logo Upload ページでアップロードすることができます。</p>
Enable Peer Loss Overlay	<p>有効になっている場合は、ネットワーク接続の消失が検出されたときに、“Network Connection Lost”オーバーレイがディスプレイ上に表示されます。このオーバーレイは VMware View などの仮想デスクトップの場合にも表示されます。通常のハイパーバイザスケジューリングの遅延によってもこのメッセージが誤ってトリガーされる場合があります。</p>

パラメータ	説明
	<p>ます。</p> <p>注意：このオプションはゼロクライアントに対してしか使用することができません。ピア消失通知が必要なデスクトップアプリケーションは、OSD、AWI、または MC を介してこの機能を再有効化する必要があります。</p>
Enable Preparing Desktop Overlay	<p>有効になっている場合は、ユーザがログインしたときに、"Preparing Desktop"オーバーレイがディスプレイ上に表示されます。</p> <p>注意：このオーバーレイは、デスクトップの表示に数秒以上かかっている場合でもログインが進行中であることを保証します。</p>
Disconnect Dialog Display Mode	<p>このフィールドを使用すれば、セッションが切断されたときに表示されるメッセージのタイプを制御することができます。次の 3 つのカテゴリに分かれています。</p> <p>情報：セッションに影響を与えるユーザまたは管理者によるアクション：</p> <ul style="list-style-type: none"> • 別の場所からログインしたか、ホストがシャットダウンまたは再起動されたために切断されました。 • 管理者が切断を実行したために切断されました。 • 別の場所からログインしたために切断されました。 • ワークステーションを切断したために切断されました。 <p>警告：セッションに影響を与えるシステムによる予想されるアクション：</p> <ul style="list-style-type: none"> • セッションがタイムアウトしたために切断されました。 <p>エラー：セッションの失敗を引き起こす予期せぬシステムによるアクション：</p> <ul style="list-style-type: none"> • 切断されました。 • 接続できません (0x1001)。IT 管理者に連絡してください。 • 接続できません (0x1002)。IT 管理者に連絡してください。 • セッションがリモートで閉じられました。 • セッションがリモートで閉じられました (原因不明)。 • 設定エラーが原因で切断されました (0x100)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x201)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x300)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x301)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x302)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x303)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x305)。IT 管理者に支援

パラメータ	説明
	<p>を要請してください。</p> <ul style="list-style-type: none"> • 設定エラーが原因で切断されました (0x400)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x401)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x402)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x403)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x404)。IT 管理者に支援を要請してください。 <p>以下の表示を選択することができます。</p> <ol style="list-style-type: none"> 1. Show All messages – このオプションは、情報メッセージ、警告メッセージ、およびエラーメッセージを含むすべての切断メッセージを表示します。 2. Show Error and Warnings Only – このオプションは情報メッセージを表示せず、エラーメッセージと警告メッセージのみを表示します。 3. Show Error Only – このオプションは情報メッセージと警告メッセージを表示せず、エラーメッセージのみを表示します。 4. Show None – どの切断メッセージも表示しません。
Session Lost Timeout	<p>アクティブセッションの接続に関するタイムアウト (秒単位) を入力します。このフィールドの有効タイムアウト範囲は 5~60 秒です。このタイムアウト期間が満了になるとセッションが切断されます。</p>

5.6.7 MC : View Connection Server + Imprivata OneSign セッション設定

クライアントが仮想デスクトップに接続するときに View Connection Server に加えて Imprivata OneSign システム経由でも認証するようにプロファイルを設定する場合は、MC で **View Connection Server + Imprivata OneSign** セッション接続タイプを選択します。

MC でプロパティを有効にするには、**Set in Profile** チェックボックスをオンにし、指示に従ってフィールドを設定します。このページでプロパティを更新したら、**Save** をクリックして変更を保存します。

この選択を変更した場合はデバイスを再起動する必要があります。

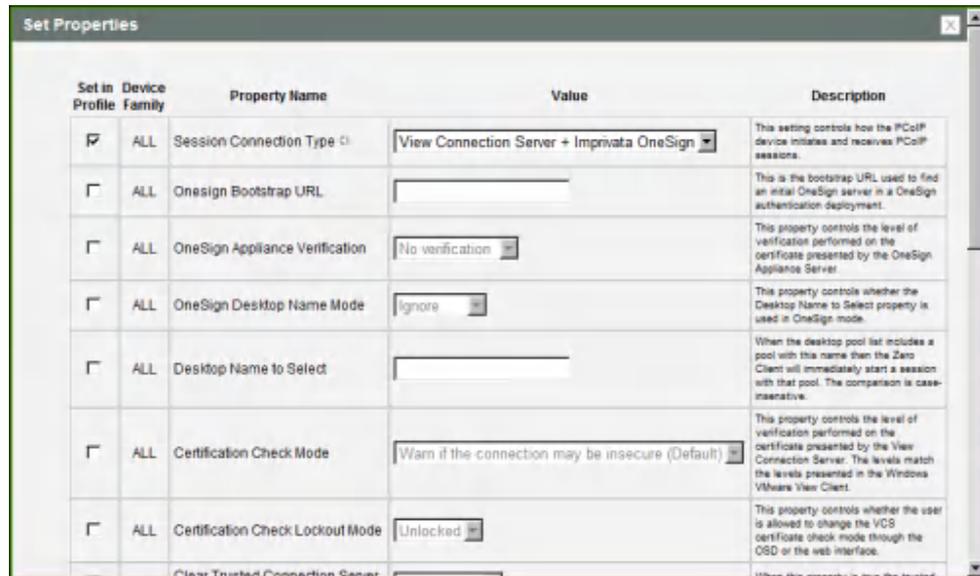


図 5-17 : MC セッション接続タイプ – View Connection Server + Imprivata OneSign

表 5-24 : MC セッション設定パラメータ

パラメータ	説明
View Connection Server Address	View Connection Server の IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。
Onesign Bootstrap URL	OneSign 認証デプロイメント内で初期 OneSign サーバを探すために使用されるブートストラップ URL を入力します。
Onesign Appliance Verification	OneSign アプライアンスサーバから提示された証明書に対して実施される検証のレベルを設定します。 <ul style="list-style-type: none"> • No verification : 任意のアプライアンスに接続します。 • Full verification : 証明書が検証済みのアプライアンスにのみ接続します。
Onesign Desktop Name Mode	Desktop Name to Select プロパティが OneSign モードで使用されるかどうかを選択します。 <ul style="list-style-type: none"> • Ignore • Use If Set
Desktop Name to Select	デスクトップ名を入力します。デスクトッププールリストにこの名前のプールが含まれている場合は、クライアントが即座にそのプールを使用したセッションを開始します。 注意：このフィールドは大文字と小文字が区別されます。
Certification Check	クライアントが View Connection Server とのセキュア接続を確認で

パラメータ	説明
Mode	<p>きない場合の動作を選択します。</p> <ul style="list-style-type: none"> • Warn if the connection may be insecure (Default) : 未署名のまたは期限切れの証明書を受信した場合、または、証明書が自己署名されておらず、ゼロクライアントのトラストストアが空の場合に警告を表示するようにクライアントを設定します（このオプションはデフォルトで選択されています）。 • Reject the unverifiable connection (Secure) : 信頼できる有効な証明書がインストールされていない場合に接続を拒否するようにクライアントを設定します。 • Allow the unverifiable connection (Not Secure) : すべての接続を許可するようにクライアントを設定します。
Certification Check Lockout Mode	<p>ユーザが OSD から VCS Certificate Check Mode 設定を変更できないようにする場合は、このプロパティを Locked に設定します。</p>
Clear Trusted Connection Server Cache	<p>有効になっている場合は、信頼できる View Connection Server のキャッシュがクリアされます。</p>
Enable Login Username Caching	<p>有効になっている場合は、ユーザ名テキストボックスに、自動的に、最後に入力されたユーザ名が設定されます。</p>
Use OSD Logo for View Banner	<p>有効になっている場合は、ログイン中に、VMware View バナーの代わりに、PCoIP ゼロクライアント OSD ロゴが表示されます。OSD ロゴは OSD Logo Upload ページでアップロードすることができます。</p>
Prefer GSC-IS Over PIV Endpoint	<p>選択されている場合は、スマートカードで CAC (GSC-IS) や PIV エンドポイントなどの複数のインターフェースがサポートされていれば、GSC-IS インターフェースが使用されます。スマートカードで CAC と PIV エンドポイントのどちらかなどの 1 つのインターフェースしかサポートされていない場合は、この設定に関係なく、CAC または PIV エンドポイントインターフェースのみが使用されます。これは、PCoIP セッション以外で実行されるスマートカードアクセスにのみ影響を与えます。</p>
Enable Peer Loss Overlay	<p>有効になっている場合は、ネットワーク接続の消失が検出されたときに、“Network Connection Lost”オーバーレイがディスプレイ上に表示されます。このオーバーレイは VMware View などの仮想デスクトップの場合にも表示されます。通常のハイパーバイザスケジューリングの遅延によってもこのメッセージが誤ってトリガーされる場合があります。</p> <p>注意：このオプションはゼロクライアントに対してしか使用することができません。ピア消失通知が必要なデスクトップアプリケーションは、OSD、AWI、または MC を介してこの機能を再有効化する必要があります。</p>

パラメータ	説明
Enable Preparing Desktop Overlay	<p>有効になっている場合は、ユーザがログインしたときに、"Preparing Desktop"オーバーレイがディスプレイ上に表示されます。</p> <p>注意：このオーバーレイは、デスクトップの表示に数秒以上かかっている場合でもログインが進行中であることを保証します。</p>
Disconnect Dialog Display Mode	<p>このフィールドを使用すれば、セッションが切断されたときに表示されるメッセージのタイプを制御することができます。次の3つのカテゴリに分かれています。</p> <p>情報：セッションに影響を与えるユーザまたは管理者によるアクション：</p> <ul style="list-style-type: none"> • 別の場所からログインしたか、ホストがシャットダウンまたは再起動されたために切断されました。 • 管理者が切断を実行したために切断されました。 • 別の場所からログインしたために切断されました。 • ワークステーションを切断したために切断されました。 <p>警告：セッションに影響を与えるシステムによる予想されるアクション：</p> <ul style="list-style-type: none"> • セッションがタイムアウトしたために切断されました。 <p>エラー：セッションの失敗を引き起こす予期せぬシステムによるアクション：</p> <ul style="list-style-type: none"> • 切断されました。 • 接続できません (0x1001)。IT 管理者に連絡してください。 • 接続できません (0x1002)。IT 管理者に連絡してください。 • セッションがリモートで閉じられました。 • セッションがリモートで閉じられました (原因不明)。 • 設定エラーが原因で切断されました (0x100)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x201)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x300)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x301)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x302)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x303)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x305)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x400)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x401)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x402)。IT 管理者に支援を要請してください。

パラメータ	説明
	<p>を要請してください。</p> <ul style="list-style-type: none"> 設定エラーが原因で切断されました (0x403)。IT 管理者に支援を要請してください。 設定エラーが原因で切断されました (0x404)。IT 管理者に支援を要請してください。 <p>以下の表示を選択することができます。</p> <ol style="list-style-type: none"> Show All messages – このオプションは、情報メッセージ、警告メッセージ、およびエラーメッセージを含むすべての切断メッセージを表示します。 Show Error and Warnings Only – このオプションは情報メッセージを表示せず、エラーメッセージと警告メッセージのみを表示します。 Show Error Only – このオプションは情報メッセージと警告メッセージを表示せず、エラーメッセージのみを表示します。 Show None – どの切断メッセージも表示しません。
Session Lost Timeout	<p>アクティブセッションの接続に関するタイムアウト (秒単位) を入力します。このフィールドの有効タイムアウト範囲は 5~60 秒です。このタイムアウト期間が満了になるとセッションが切断されます。</p>

5.6.8 MC : Connection Management Interface 設定

外部コネクションマネージャを [コネクションブローカ](#) として使用するようプロファイルを設定する場合は、MC で **Connection Management Interface** セッション接続タイプを選択します。

注意：外部コネクションマネージャは大規模で複雑なシステムの管理手順を簡略化することができます。管理接続では、外部コネクションマネージャサーバがデバイスと通信して、それをリモートで制御および設定することができます。コネクションマネージャは、接続するデバイスに適切なピアを特定してから接続を開始することもできます。

MC でプロパティを有効にするには、**Set in Profile** チェックボックスをオンにし、指示に従ってフィールドを設定します。このページでプロパティを更新したら、**Save** をクリックして変更を保存します。

この選択を変更した場合はデバイスを再起動する必要があります。

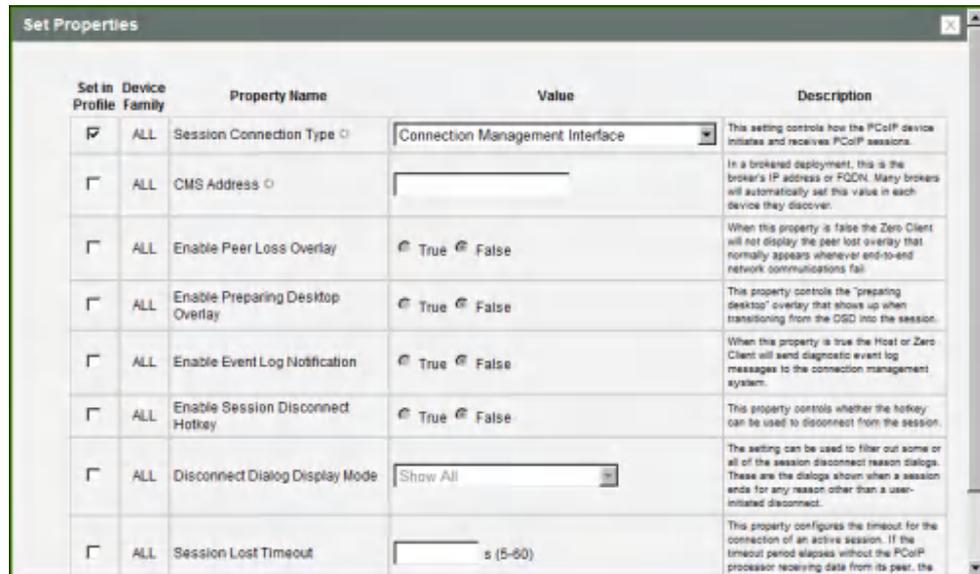


図 5-18 : MC セッション接続タイプ – Connection Management Interface

表 5-25 : MC セッション設定パラメータ

パラメータ	説明
CMS Address	コネクションマネージャの IP アドレスまたは完全修飾ドメイン名 (FQDN) を入力します。 注意：多くのコネクションマネージャが、自動的に、発見したすべてのデバイスにこの値を設定します。
Enable Peer Loss Overlay	有効になっている場合は、ネットワーク接続の消失が検出されたときに、“Network Connection Lost”オーバーレイがディスプレイ上に表示されます。このオーバーレイは VMware View などの仮想デスクトップの場合にも表示されます。通常のハイパーバイザスケジューリングの遅延によってもこのメッセージが誤ってトリガーされる場合があります。 注意：このオプションはゼロクライアントに対してしか使用することができません。ピア消失通知が必要なデスクトップアプリケーションは、OSD、AWI、または MC を介してこの機能を再有効化する必要があります。
Enable Preparing Desktop Overlay	有効になっている場合は、ユーザがログインしたときに、“Preparing Desktop”オーバーレイがディスプレイ上に表示されます。 注意：このオーバーレイは、デスクトップの表示に数秒以上かかっている場合でもログインが進行中であることを保証します。
Disconnect Dialog Display Mode	このフィールドを使用すれば、セッションが切断されたときに表示されるメッセージのタイプを制御することができます。次の 3 つのカテゴリに分かれています。

パラメータ	説明
	<p>情報：セッションに影響を与えるユーザまたは管理者によるアクション：</p> <ul style="list-style-type: none"> • 別の場所からログインしたか、ホストがシャットダウンまたは再起動されたために切断されました。 • 管理者が切断を実行したために切断されました。 • 別の場所からログインしたために切断されました。 • ワークステーションを切断したために切断されました。 <p>警告：セッションに影響を与えるシステムによる予想されるアクション：</p> <ul style="list-style-type: none"> • セッションがタイムアウトしたために切断されました。 <p>エラー：セッションの失敗を引き起こす予期せぬシステムによるアクション：</p> <ul style="list-style-type: none"> • 切断されました。 • 接続できません (0x1001)。IT 管理者に連絡してください。 • 接続できません (0x1002)。IT 管理者に連絡してください。 • セッションがリモートで閉じられました。 • セッションがリモートで閉じられました (原因不明)。 • 設定エラーが原因で切断されました (0x100)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x201)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x300)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x301)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x302)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x303)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x305)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x400)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x401)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x402)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x403)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x404)。IT 管理者に支援を要請してください。 <p>以下の表示を選択することができます。</p> <p>1. Show All messages – このオプションは、情報メッセージ、警告メッセージ、およびエラーメッセージを含むすべての切断メッセ</p>

パラメータ	説明
	ージを表示します。 2. Show Error and Warnings Only – このオプションは情報メッセージを表示せず、エラーメッセージと警告メッセージのみを表示します。 3. Show Error Only – このオプションは情報メッセージと警告メッセージを表示せず、エラーメッセージのみを表示します。 4. Show None – どの切断メッセージも表示しません。
Session Lost Timeout	アクティブセッションの接続に関するタイムアウト（秒単位）を入力します。このフィールドの有効タイムアウト範囲は 5~60 秒です。このタイムアウト期間が満了になるとセッションが切断されます。

5.6.9 AWI ホスト : Direct from Client セッション設定

クライアントに直接接続するようにホストを設定する場合は、**Configuration > Session** ページで **Direct from Client** セッション接続タイプを選択します。

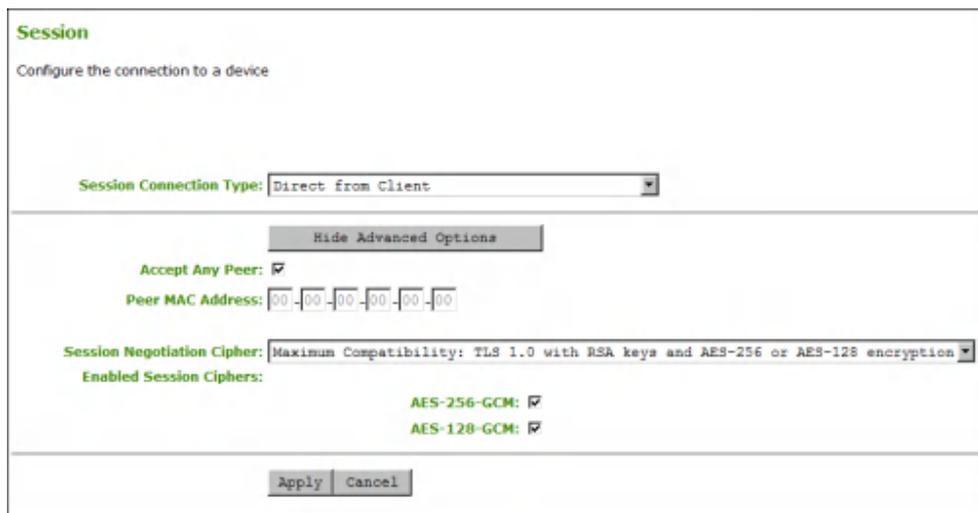


図 5-19 : AWI セッション接続タイプ – Direct from Client

表 5-26 : AWI Session ページパラメータ

パラメータ	説明
Accept Any Peer	有効になっている場合は、ホストが任意のクライアントからの接続を受け入れます。無効になっている場合は、ホストに受け入れさせるピアの MAC アドレスを指定する必要があります。
Peer MAC Address	ホストへの接続を許可するクライアントの MAC アドレスを入力します。 Accept Any Peer オプションが有効になっている場合は、このフィールドが不要なため、編集不可になります。

パラメータ	説明
Session Negotiation Cipher	<p>クライアントが PCoIP クライアントと PCoIP ホスト間のトランスポート層セキュリティ (TLS) セッションをネゴシエートするために使用する TLS 暗号を設定します。</p> <ul style="list-style-type: none"> • TLS 1.0 with RSA keys and AES-256 or AES-128 encryption : このオプションは最大限の互換性を提供します。 • TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption : このオプションはより高度なセキュリティを提供します。
Enabled Session Ciphers	<p>デバイスの暗号化モードを有効または無効にします。デフォルトで、デバイスに関係するすべての暗号化モードが有効になっています。</p> <ul style="list-style-type: none"> • AES-128-GCM (Tera1 と Tera2) : 第 1 世代 Tera1 プロセッサと第 2 世代 Tera2 プロセッサに実装されている暗号化方式。この方式では、Tera1 デバイスのハードウェアエンドポイント間で最高性能を実現することができます。また、Tera2 クライアントが VMware 4 以降に接続されており、ネットワーク上で 7 Mbps 以上の速度が利用可能であれば、高い性能を実現できる可能性があります。 • AES-256-GCM (Tera2 のみ) : 第 2 世代 Tera2 プロセッサに実装されているよりセキュアな暗号化方式で、ハードウェアエンドポイント間で最高性能を実現することができます。VMware 4 以降に接続されている場合は、AES-128-GCM をお勧めします。 • Salsa20-256-Round12 (Tera1 のみ) : Tera1 クライアントが VMware 4 以降に接続されており、ネットワーク上で 7 Mbps 以上の速度が利用可能であれば、高い性能を実現することが可能な、ファームウェアに実装されているより軽量な暗号化方式。 <p>注意 : VMware View 仮想デスクトップへの接続方法については、『Using PCoIP Zero Clients with VMware View User Guide』(TER0904005) を参照してください。</p> <p>注意 : 有効にする暗号化モードは、セッションを確立するホストとクライアント間で一致させる必要があります。複数のモードが有効になっている場合は、ファームウェアが次のように選択します。</p> <ul style="list-style-type: none"> • ホストと Tera1 または Tera2 クライアント間 : PCoIP セッションに対して AES-128-GCM または AES-256-GCM • VMware View 4.5 以降と Tera1 クライアント間 : PCoIP セッションに対して SALSA20-256-Round12 • VMware View 4.5 以降と Tera2 クライアント間 : PCoIP セッションに対して AES-128-GCM

5.6.10 AWI クライアント : Direct to Host セッション設定

ホストに直接接続するようにクライアントを設定する場合は、**Configuration > Session** ページで **Direct to Host** セッション接続タイプを選択します。

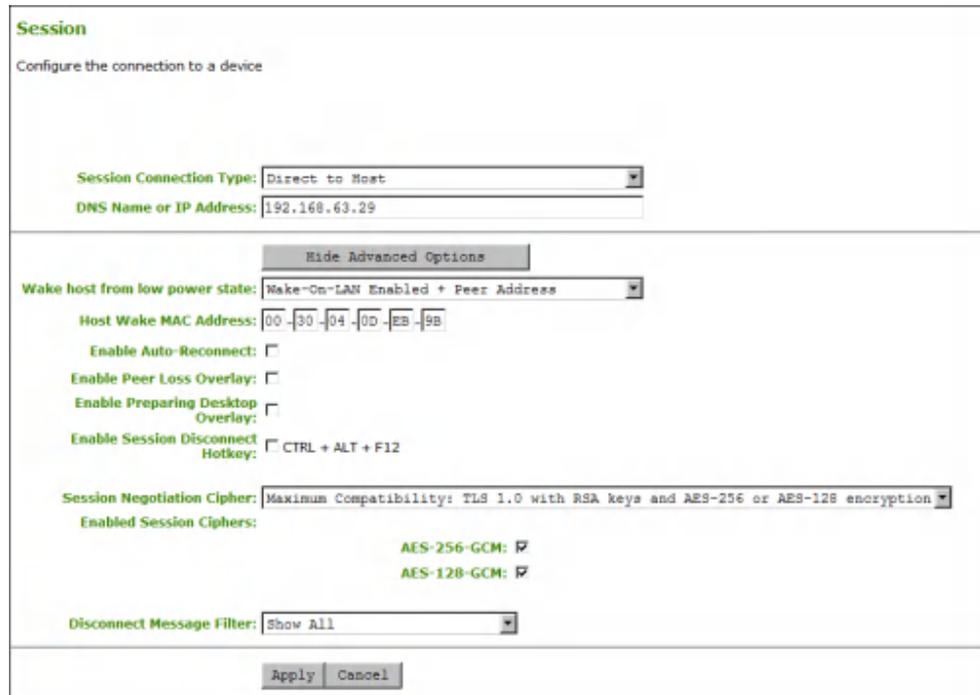


図 5-20 : AWI セッション接続タイプ – Direct to Host

表 5-27 : AWI Session ページパラメータ

パラメータ	説明
DNS Name or IP Address	ホストの IP アドレスまたは DNS 名を入力します。
Wake host from low power state	<p>ユーザがクライアントのリモート PC ボタンを押すか、Connect ウィンドウの Connect ボタンをクリックしたときに、自動的に、クライアントからホストを再開させるかどうかを設定します。</p> <ul style="list-style-type: none"> • Wake-On-LAN Disabled : 選択されている場合は、再開機能が無効になります。このオプションはデフォルトで選択されています。 • Wake-On-LAN Enabled + Peer Address : 選択されている場合は、再開機能が有効になり、Host Wake MAC Address フィールドが表示され、ホストの MAC アドレスを入力することができます。このオプションは、クライアントとホストが同じネットワークに接続されている場合に使用します。 • Wake-On-LAN Enabled + Custom Address : 選択されている場合は、再開機能が有効になり、Host Wake MAC Address フィールドと Host Wake IP Address フィールドが表示され、ホストの両方のアドレスを入力できるようになります。このオプションは、ホストがクライアントとは別のネットワークに接続されている場合に選択します。 <p>注意 :</p> <ul style="list-style-type: none"> • この機能はハードウェアホストでのみ動作します。低電力状態に

パラメータ	説明
	<p>入ることができないため、ソフトウェアホストでは動作しません。</p> <ul style="list-style-type: none"> ハードウェアホストは、Wake-on-LAN パケットを受信したときに低電力状態（オフ/休止/スリープ）からの再開をサポートする必要があります。
Host Wake MAC Address	<p>Wake-On-LAN Enabled + Peer Address または Wake-On-LAN Enabled + Custom Address が選択されている場合に、ホスト再開設定を完成させるためのホストの MAC アドレスを入力します。クライアントは、ホストを低電力状態から再開させるために、この MAC アドレスに「マジックパケット」を送信します。</p>
Host Wake IP Address	<p>Wake-On-LAN Enabled + Custom Address が選択されている場合に、ホスト再開設定を完成させるためのホストの IP アドレスを入力します。クライアントは、ホストコンピュータを低電力状態から再開させるために、この IP アドレスに「マジックパケット」を送信します。</p>
Enable Auto-Reconnect	<p>有効になっている場合は、セッションが失われたときに、クライアントが自動的に最後に接続していたホストに再接続します。</p>
Enable Peer Loss Overlay	<p>有効になっている場合は、ネットワーク接続の消失が検出されたときに、“Network Connection Lost”オーバーレイがディスプレイ上に表示されます。このオーバーレイは VMware View などの仮想デスクトップの場合にも表示されます。通常のハイパーバイザスケジューリングの遅延によってもこのメッセージが誤ってトリガーされる場合があります。</p> <p>注意：このオプションはゼロクライアントに対してしか使用することができません。ピア消失通知が必要なデスクトップアプリケーションは、OSD、AWI、または MC を介してこの機能を再有効化する必要があります。</p>
Enable Preparing Desktop Overlay	<p>有効になっている場合は、ユーザがログインしたときに、“Preparing Desktop”オーバーレイがディスプレイ上に表示されます。</p> <p>注意：このオーバーレイは、デスクトップの表示に数秒以上かかっている場合でもログインが進行中であることを保証します。</p>
Enable Session Disconnect Hotkey	<p>有効になっている場合は、ユーザが Ctrl+Alt+F12 ホットキーシーケンスを押すと、“Zero Client Control Panel”オーバーレイがポップアップ表示されます。ここで、ユーザはワークステーション上の現在のセッションを切断したり、ワークステーションの電源をオフにしたりすることができます。</p> <p>注意：ユーザがこの切断ホットキーシーケンスを使用できるようにするには、他の特定の設定オプションを有効にする必要があります。詳細については、「セッションの切断」を参照してください。</p>

パラメータ	説明
Session Negotiation Cipher	<p>クライアントが PCoIP クライアントと PCoIP ホスト間のトランスポート層セキュリティ (TLS) セッションをネゴシエートするために使用する TLS 暗号を設定します。</p> <ul style="list-style-type: none"> TLS 1.0 with RSA keys and AES-256 or AES-128 encryption : このオプションは最大限の互換性を提供します。 TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption : このオプションはより高度なセキュリティを提供します。
Enabled Session Ciphers	<p>デバイスの暗号化モードを有効または無効にします。デフォルトで、デバイスに関するすべての暗号化モードが有効になっています。</p> <ul style="list-style-type: none"> AES-128-GCM (Tera1 と Tera2) : 第 1 世代 Tera1 プロセッサと第 2 世代 Tera2 プロセッサに実装されている暗号化方式。この方式では、Tera1 デバイスのハードウェアエンドポイント間で最高性能を実現することができます。また、Tera2 クライアントが VMware 4 以降に接続されており、ネットワーク上で 7 Mbps 以上の速度が利用可能であれば、高い性能を実現できる可能性があります。 AES-256-GCM (Tera2 のみ) : 第 2 世代 Tera2 プロセッサに実装されているよりセキュアな暗号化方式で、ハードウェアエンドポイント間で最高性能を実現することができます。VMware 4 以降に接続されている場合は、AES-128-GCM をお勧めします。 Salsa20-256-Round12 (Tera1 のみ) : Tera1 クライアントが VMware 4 以降に接続されており、ネットワーク上で 7 Mbps 以上の速度が利用可能であれば、高い性能を実現することが可能な、ファームウェアに実装されているより軽量な暗号化方式。 <p>注意 : VMware View 仮想デスクトップへの接続方法については、『Using PCoIP Zero Clients with VMware View User Guide』(TER0904005) を参照してください。</p> <p>注意 : 有効にする暗号化モードは、セッションを確立するホストとクライアント間で一致させる必要があります。複数のモードが有効になっている場合は、ファームウェアが次のように選択します。</p> <ul style="list-style-type: none"> ホストと Tera1 または Tera2 クライアント間 : PCoIP セッションに対して AES-128-GCM または AES-256-GCM VMware View 4.5 以降と Tera1 クライアント間 : PCoIP セッションに対して SALSA20-256-Round12 VMware View 4.5 以降と Tera2 クライアント間 : PCoIP セッションに対して AES-128-GCM
Disconnect Message Filter	<p>このフィールドを使用すれば、セッションが切断されたときに表示されるメッセージのタイプを制御することができます。次の 3 つのカテゴリに分かれています。</p> <p>情報 : セッションに影響を与えるユーザまたは管理者によるアクション :</p> <ul style="list-style-type: none"> 別の場所からログインしたか、ホストがシャットダウンまたは再起動されたために切断されました。

パラメータ	説明
	<ul style="list-style-type: none"> • 管理者が切断を実行したために切断されました。 • 別の場所からログインしたために切断されました。 • ワークステーションを切断したために切断されました。 <p>警告：セッションに影響を与えるシステムによる予想されるアクション：</p> <ul style="list-style-type: none"> • セッションがタイムアウトしたために切断されました。 <p>エラー：セッションの失敗を引き起こす予期せぬシステムによるアクション：</p> <ul style="list-style-type: none"> • 切断されました。 • 接続できません (0x1001)。IT 管理者に連絡してください。 • 接続できません (0x1002)。IT 管理者に連絡してください。 • セッションがリモートで閉じられました。 • セッションがリモートで閉じられました (原因不明)。 • 設定エラーが原因で切断されました (0x100)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x201)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x300)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x301)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x302)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x303)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x305)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x400)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x401)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x402)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x403)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x404)。IT 管理者に支援を要請してください。 <p>以下の表示を選択することができます。</p> <ol style="list-style-type: none"> 1. Show All messages – このオプションは、情報メッセージ、警告メッセージ、およびエラーメッセージを含むすべての切断メッセージを表示します。 2. Show Error and Warnings Only – このオプションは情報メッセージを表示せず、エラーメッセージと警告メッセージのみを表示します。

パラメータ	説明
	3. Show Error Only – このオプションは情報メッセージと警告メッセージを表示せず、エラーメッセージのみを表示します。 4. Show None – どの切断メッセージも表示しません。

5.6.11 AWI クライアント : Direct to Host + SLP ホストディスカバリセッション設定

ホストに直接接続したり、サービスローションプロトコル (SLP) 経由で自動的にホストを発見したりするようにクライアントを設定する場合は、**Configuration > Session** ページで **Direct to Host + SLP ホストディスカバリセッション接続タイプ** を選択します。

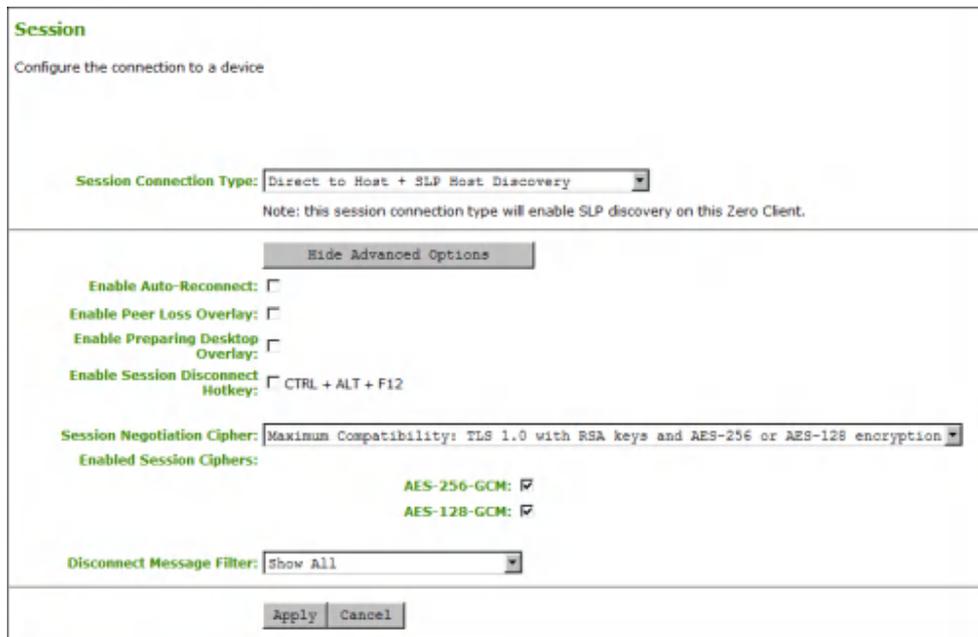


図 5-21 : AWI セッション接続タイプ – Direct to Host + SLP ホストディスカバリ

表 5-28 : AWI Session ページパラメータ

パラメータ	説明
Enable Auto-Reconnect	有効になっている場合は、セッションが失われたときに、クライアントが自動的に最後に接続していたホストに再接続します。
Enable Peer Loss Overlay	有効になっている場合は、ネットワーク接続の消失が検出されたときに、“Network Connection Lost”オーバーレイがディスプレイ上に表示されます。このオーバーレイは VMware View などの仮想デスクトップ

パラメータ	説明
	<p>プの場合にも表示されます。通常のハイパーバイザスケジューリングの遅延によってもこのメッセージが誤ってトリガーされる場合があります。</p> <p>注意：このオプションはゼロクライアントに対してしか使用することができません。ピア消失通知が必要なデスクトップアプリケーションは、OSD、AWI、またはMCを介してこの機能を再有効化する必要があります。</p>
<p>Enable Preparing Desktop Overlay</p>	<p>有効になっている場合は、ユーザがログインしたときに、"Preparing Desktop"オーバーレイがディスプレイ上に表示されます。</p> <p>注意：このオーバーレイは、デスクトップの表示に数秒以上かかっている場合でもログインが進行中であることを保証します。</p>
<p>Enable Session Disconnect Hotkey</p>	<p>有効になっている場合は、ユーザが Ctrl+Alt+F12 ホットキーシーケンスを押すと、"Zero Client Control Panel"オーバーレイがポップアップ表示されます。ここで、ユーザはワークステーション上の現在のセッションを切断したり、ワークステーションの電源をオフにしたりすることができます。</p> <p>注意：ユーザがこの切断ホットキーシーケンスを使用できるようにするには、他の特定の設定オプションを有効にする必要があります。詳細については、「セッションの切断」を参照してください。</p>
<p>Session Negotiation Cipher</p>	<p>クライアントが PCoIP クライアントと PCoIP ホスト間のトランスポート層セキュリティ (TLS) セッションをネゴシエートするために使用する TLS 暗号を設定します。</p> <ul style="list-style-type: none"> ● TLS 1.0 with RSA keys and AES-256 or AES-128 encryption : このオプションは最大限の互換性を提供します。 ● TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption : このオプションはより高度なセキュリティを提供します。
<p>Enabled Session Ciphers</p>	<p>デバイスの暗号化モードを有効または無効にします。デフォルトで、デバイスに関係するすべての暗号化モードが有効になっています。</p> <ul style="list-style-type: none"> ● AES-128-GCM (Tera1 と Tera2) : 第1世代 Tera1 プロセッサと第2世代 Tera2 プロセッサに実装されている暗号化方式。この方式では、Tera1 デバイスのハードウェアエンドポイント間で最高性能を実現することができます。また、Tera2 クライアントが VMware 4 以降に接続されており、ネットワーク上で 7 Mbps 以上の速度が利用可能であれば、高い性能を実現できる可能性があります。 ● AES-256-GCM (Tera2 のみ) : 第2世代 Tera2 プロセッサに実装されているよりセキュアな暗号化方式で、ハードウェアエンドポイント間で最高性能を実現することができます。VMware 4 以降に接続されている場合は、AES-128-GCM をお勧めします。 ● Salsa20-256-Round12 (Tera1 のみ) : Tera1 クライアントが VMware 4 以降に接続されており、ネットワーク上で 7 Mbps 以上

パラメータ	説明
	<p>の速度が利用可能であれば、高い性能を実現することが可能な、ファームウェアに実装されているより軽量の暗号化方式。</p> <p>注意：VMware View 仮想デスクトップへの接続方法については、『Using PCoIP Zero Clients with VMware View User Guide』（TER0904005）を参照してください。</p> <p>注意：有効にする暗号化モードは、セッションを確立するホストとクライアント間で一致させる必要があります。複数のモードが有効になっている場合は、ファームウェアが次のように選択します。</p> <ul style="list-style-type: none"> • ホストと Tera1 または Tera2 クライアント間：PCoIP セッションに対して AES-128-GCM または AES-256-GCM • VMware View 4.5 以降と Tera1 クライアント間：PCoIP セッションに対して SALSA20-256-Round12 • VMware View 4.5 以降と Tera2 クライアント間：PCoIP セッションに対して AES-128-GCM
Disconnect Message Filter	<p>このフィールドを使用すれば、セッションが切断されたときに表示されるメッセージのタイプを制御することができます。次の 3 つのカテゴリに分かれています。</p> <p>情報：セッションに影響を与えるユーザまたは管理者によるアクション：</p> <ul style="list-style-type: none"> • 別の場所からログインしたか、ホストがシャットダウンまたは再起動されたために切断されました。 • 管理者が切断を実行したために切断されました。 • 別の場所からログインしたために切断されました。 • ワークステーションを切断したために切断されました。 <p>警告：セッションに影響を与えるシステムによる予想されるアクション：</p> <ul style="list-style-type: none"> • セッションがタイムアウトしたために切断されました。 <p>エラー：セッションの失敗を引き起こす予期せぬシステムによるアクション：</p> <ul style="list-style-type: none"> • 切断されました。 • 接続できません (0x1001)。IT 管理者に連絡してください。 • 接続できません (0x1002)。IT 管理者に連絡してください。 • セッションがリモートで閉じられました。 • セッションがリモートで閉じられました (原因不明)。 • 設定エラーが原因で切断されました (0x100)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x201)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x300)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x301)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x302)。IT 管理者に支援

パラメータ	説明
	<p>を要請してください。</p> <ul style="list-style-type: none"> • 設定エラーが原因で切断されました (0x303)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x305)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x400)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x401)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x402)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x403)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x404)。IT 管理者に支援を要請してください。 <p>以下の表示を選択することができます。</p> <ol style="list-style-type: none"> 1. Show All messages – このオプションは、情報メッセージ、警告メッセージ、およびエラーメッセージを含むすべての切断メッセージを表示します。 2. Show Error and Warnings Only – このオプションは情報メッセージを表示せず、エラーメッセージと警告メッセージのみを表示します。 3. Show Error Only – このオプションは情報メッセージと警告メッセージを表示せず、エラーメッセージのみを表示します。 4. Show None – どの切断メッセージも表示しません。

5.6.12 AWI クライアント : View Connection Server セッション設定

VMware View Connection Server を使用して仮想デスクトップに接続するようにクライアントを設定する場合は、**Configuration > Session** ページで **View Connection Server** セッション接続タイプを選択します。

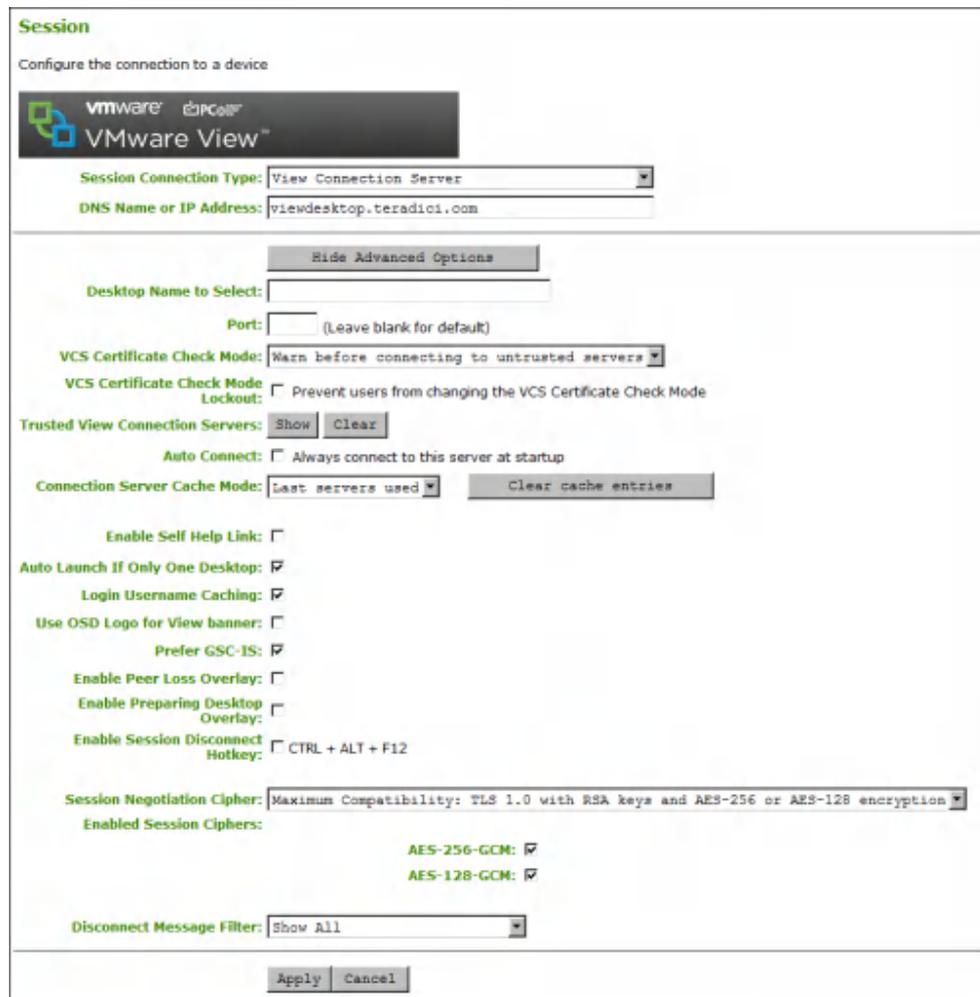


図 5-22 : AWI セッション接続タイプ – View Connection Server

表 5-29 : AWI Session ページパラメータ

パラメータ	説明
DNS Name or IP Address	VMware View Connection Server の DNS 名または IP アドレスを入力します。
Desktop Name to Select	セッションを開始するときにクライアントが使用するプール/デスクトップ名を入力します。 注意：この設定は省略可能です。
Port	デフォルトで、このフィールドは空白になっており、View Connection Server との通信にはポート 443 が使用されます。ネットワークがセキュア接続用として非標準ポートを使用するようにセットアップされている場合は、ポート番号を入力します。

パラメータ	説明
VCS Certificate Check Mode	<p>クライアントが View Connection Server とのセキュア接続を確認できない場合の動作を選択します。</p> <ul style="list-style-type: none"> • Never connect to untrusted servers : 信頼できる有効な証明書がインストールされていない場合に接続を拒否するようにクライアントを設定します (これは最もセキュアなオプションです)。 • Warn before connecting to untrusted servers : 未署名のまたは期限切れの証明書を受信した場合、または、証明書が自己署名されておらず、ゼロクライアントのトラストストアが空の場合に警告を表示するようにクライアントを設定します (このオプションはデフォルトで選択されています)。 • Do not verify server identity certificates : すべての接続を許可するようにクライアントを設定します (このオプションはセキュアではありません)。
VCS Certificate Check Mode Lockout	<p>ユーザが OSD から VCS Certificate Check Mode 設定を変更できないようにします。</p>
Trusted View Connection Servers	<p>Show ボタンをクリックすると、クライアントが有効な証明書を受信した VMware View Connection Server が表示されます。</p> <p>Clear ボタンをクリックすると、このキャッシュがクリアされます。</p>
Auto Connect	<p>有効になっている場合は、クライアントが、電源がオンになっているときはいつでも、または、仮想デスクトップとのセッションが終了したときに、自動的に、選択された View Connection Server に接続します。</p> <p>注意 : Auto Connect を有効にしたら、変更を反映させるためにクライアントの電源を入れ直す必要があります。</p>
Connection Server Cache Mode	<p>このフィールドは、ユーザが有効なサーバアドレスを入力したときに View Connection Server を OSD Connect ページの Server ドロップダウンメニューに動的に追加するかどうか、または、ユーザが選択するための読み取り専用リストに View Connection Server を表示するかどうかを決定します。</p> <ul style="list-style-type: none"> • Last servers used : ユーザが入力したキャッシュサーバのリストを OSD Connect ページの Server ドロップダウンメニューに表示したい場合にこのオプションを選択します。 • Read-only : ユーザに読み取り専用リストから View Connection Server を選択させたい場合にこのオプションを選択します。 <p>注意 : PCoIP 管理コンソールを使用して、使用可能なコネクションサーバのリストを事前に生成しておくことができます。</p>
Enable Self Help Link	<p>詳細については、「セルフヘルプリンクの有効化」を参照してください。</p>
Auto Launch If Only One	<p>有効になっている場合は、ユーザ資格情報の入力後に、自動的に、ユ</p>

パラメータ	説明
Desktop	<p>ユーザが仮想デスクトップに接続されます。</p> <p>注意：この機能は、単一のデスクトップを使用可能なユーザにのみ適用されます。複数の仮想デスクトップを使用可能なユーザには適用されません。</p>
Login Username Caching	<p>有効になっている場合は、ユーザ名テキストボックスに、自動的に、最後に入力されたユーザ名が設定されます。</p>
Use OSD Logo for View Banner	<p>有効になっている場合は、ログイン中に、VMware View バナーの代わりに、PCoIP ゼロクライアント OSD ロゴが表示されます。OSD ロゴは OSD Logo Upload ページでアップロードすることができます。</p>
Prefer GSC-IS	<p>選択されている場合は、スマートカードで CAC (GSC-IS) や PIV エンドポイントなどの複数のインターフェースがサポートされている場合、GSC-IS インターフェースが使用されます。スマートカードで CAC と PIV エンドポイントのどちらかなどの 1 つのインターフェースしかサポートされていない場合は、この設定に関係なく、CAC または PIV エンドポイントインターフェースのみが使用されます。これは、PCoIP セッション以外で実行されるスマートカードアクセスのみ影響を与えます。</p>
Enable Peer Loss Overlay	<p>有効になっている場合は、ネットワーク接続の消失が検出されたときに、“Network Connection Lost”オーバーレイがディスプレイ上に表示されます。このオーバーレイは VMware View などの仮想デスクトップの場合にも表示されます。通常のハイパーバイザスケジューリングの遅延によってもこのメッセージが誤ってトリガーされる場合があります。</p> <p>注意：このオプションはゼロクライアントに対してしか使用することができません。ピア消失通知が必要なデスクトップアプリケーションは、OSD、AWI、または MC を介してこの機能を再有効化する必要があります。</p>
Enable Preparing Desktop Overlay	<p>有効になっている場合は、ユーザがログインしたときに、“Preparing Desktop”オーバーレイがディスプレイ上に表示されます。</p> <p>注意：このオーバーレイは、デスクトップの表示に数秒以上かかっている場合でもログインが進行中であることを保証します。</p>
Enable Session Disconnect Hotkey	<p>有効になっている場合は、ユーザが Ctrl+Alt+F12 ホットキーシーケンスを押すと、“Zero Client Control Panel”オーバーレイがポップアップ表示されます。ここで、ユーザはワークステーション上の現在のセッションを切断したり、ワークステーションの電源をオフにしたりすることができます。</p> <p>注意：ユーザがこの切断ホットキーシーケンスを使用できるようにするには、他の特定の設定オプションを有効にする必要があります。詳細については、「セッションの切断」を参照してください。</p>

パラメータ	説明
Session Negotiation Cipher	<p>クライアントが PCoIP クライアントと PCoIP ホスト間のトランスポート層セキュリティ (TLS) セッションをネゴシエートするために使用する TLS 暗号を設定します。</p> <ul style="list-style-type: none"> • TLS 1.0 with RSA keys and AES-256 or AES-128 encryption : このオプションは最大限の互換性を提供します。 • TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption : このオプションはより高度なセキュリティを提供します。
Enabled Session Ciphers	<p>デバイスの暗号化モードを有効または無効にします。デフォルトで、デバイスに関するすべての暗号化モードが有効になっています。</p> <ul style="list-style-type: none"> • AES-128-GCM (Tera1 と Tera2) : 第 1 世代 Tera1 プロセッサと第 2 世代 Tera2 プロセッサに実装されている暗号化方式。この方式では、Tera1 デバイスのハードウェアエンドポイント間で最高性能を実現することができます。また、Tera2 クライアントが VMware 4 以降に接続されており、ネットワーク上で 7 Mbps 以上の速度が利用可能であれば、高い性能を実現できる可能性があります。 • AES-256-GCM (Tera2 のみ) : 第 2 世代 Tera2 プロセッサに実装されているよりセキュアな暗号化方式で、ハードウェアエンドポイント間で最高性能を実現することができます。VMware 4 以降に接続されている場合は、AES-128-GCM をお勧めします。 • Salsa20-256-Round12 (Tera1 のみ) : Tera1 クライアントが VMware 4 以降に接続されており、ネットワーク上で 7 Mbps 以上の速度が利用可能であれば、高い性能を実現することが可能な、ファームウェアに実装されているより軽量な暗号化方式。 <p>注意 : VMware View 仮想デスクトップへの接続方法については、『Using PCoIP Zero Clients with VMware View User Guide』(TER0904005) を参照してください。</p> <p>注意 : 有効にする暗号化モードは、セッションを確立するホストとクライアント間で一致させる必要があります。複数のモードが有効になっている場合は、ファームウェアが次のように選択します。</p> <ul style="list-style-type: none"> • ホストと Tera1 または Tera2 クライアント間 : PCoIP セッションに対して AES-128-GCM または AES-256-GCM • VMware View 4.5 以降と Tera1 クライアント間 : PCoIP セッションに対して SALSA20-256-Round12 • VMware View 4.5 以降と Tera2 クライアント間 : PCoIP セッションに対して AES-128-GCM
Disconnect Message Filter	<p>このフィールドを使用すれば、セッションが切断されたときに表示されるメッセージのタイプを制御することができます。次の 3 つのカテゴリに分かれています。</p> <p>情報 : セッションに影響を与えるユーザまたは管理者によるアクション :</p> <ul style="list-style-type: none"> • 別の場所からログインしたか、ホストがシャットダウンまたは再起動されたために切断されました。

パラメータ	説明
	<ul style="list-style-type: none"> • 管理者が切断を実行したために切断されました。 • 別の場所からログインしたために切断されました。 • ワークステーションを切断したために切断されました。 <p>警告：セッションに影響を与えるシステムによる予想されるアクション：</p> <ul style="list-style-type: none"> • セッションがタイムアウトしたために切断されました。 <p>エラー：セッションの失敗を引き起こす予期せぬシステムによるアクション：</p> <ul style="list-style-type: none"> • 切断されました。 • 接続できません (0x1001)。IT 管理者に連絡してください。 • 接続できません (0x1002)。IT 管理者に連絡してください。 • セッションがリモートで閉じられました。 • セッションがリモートで閉じられました (原因不明)。 • 設定エラーが原因で切断されました (0x100)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x201)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x300)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x301)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x302)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x303)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x305)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x400)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x401)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x402)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x403)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x404)。IT 管理者に支援を要請してください。 <p>以下の表示を選択することができます。</p> <ol style="list-style-type: none"> 1. Show All messages – このオプションは、情報メッセージ、警告メッセージ、およびエラーメッセージを含むすべての切断メッセージを表示します。 2. Show Error and Warnings Only – このオプションは情報メッセージを表示せず、エラーメッセージと警告メッセージのみを表示します。

パラメータ	説明
	3. Show Error Only – このオプションは情報メッセージと警告メッセージを表示せず、エラーメッセージのみを表示します。 4. Show None – どの切断メッセージも表示しません。

セルフヘルプリンクの有効化

Self Help Link オプションを使用すれば、ユーザのセルフヘルプリンクを **Connect** ウィンドウに表示するように設定することができます。ログオン詳細を設定すると、ユーザがセルフヘルプリンクをクリックしたときに自動的に仮想マシンにログインすることが保証されます。

図 5-23 : Self Help Link オプションの有効化

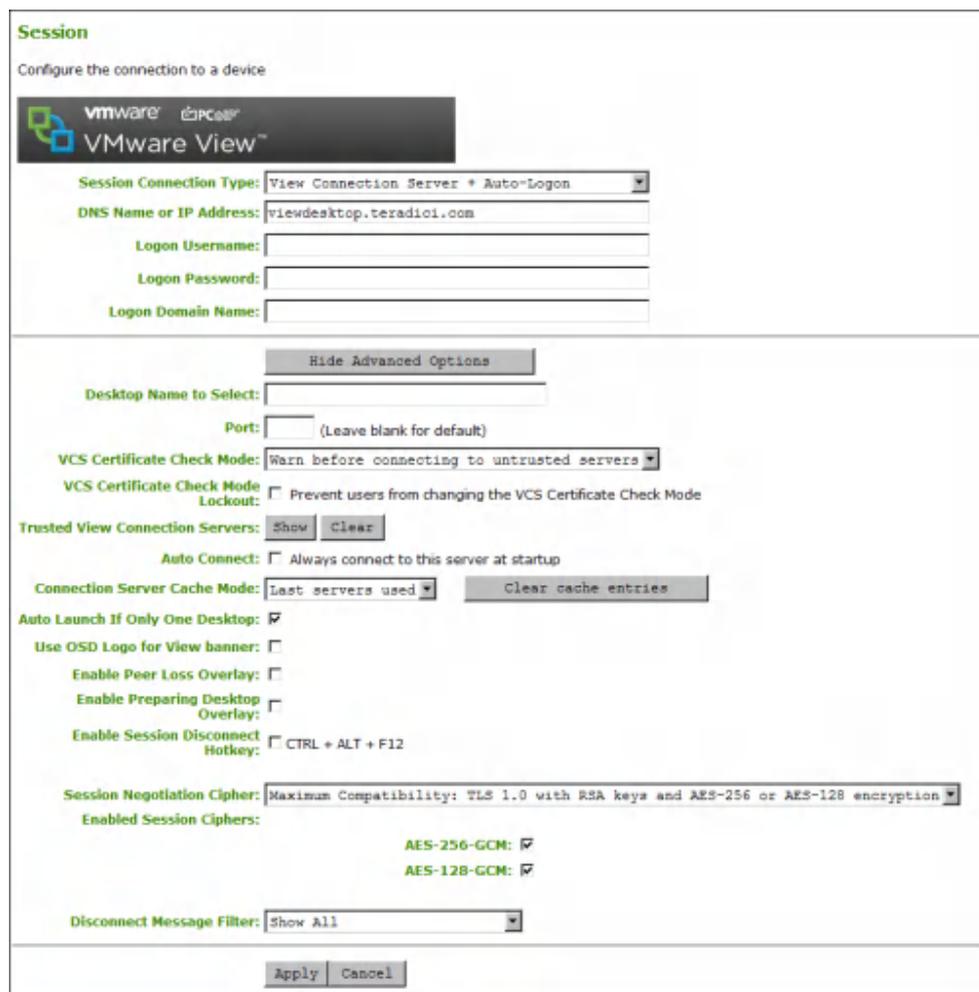
このフィールドを有効にすると、次のようなオプションが表示されます。

パラメータ	説明
View Connection Server	セルフヘルプ仮想マシンをホストしている View Connection Server の名前を入力します。
Port	デフォルトで、このフィールドは空白になっており、View Connection Server との通信にはポート 443 が使用されます。ネットワークがセキュア接続用として非標準ポートを使用するようにセットアップされている場合は、ポート番号を入力します。
Username	セルフヘルプリンクに対して仮想マシンをパスワードで保護する場合に、このフィールドにユーザ名を入力します。
Password	セルフヘルプリンクに対して仮想マシンをパスワードで保護する場合に、このフィールドにパスワードを入力します。
Domain	セルフヘルプリンクの仮想マシンで使用されるドメイン名を入力します。

パラメータ	説明
Desktop Name to Select	セルフヘルプリンクの仮想マシンで使用されるプール/デスクトップ名を入力します。
Link Text	Connect ウィンドウにハイパーリンクとして表示するテキストを入力します。

5.6.13 AWI クライアント : View Connection Server + 自動ログインセッション設定

ユーザが VMware View Connection Server 経由で仮想デスクトップに接続するときに自動的にユーザのログイン詳細を入力するようにクライアントを設定する場合は、**Configuration > Session** ページで **View Connection Server + 自動ログインセッション** 接続タイプを選択します。



The screenshot shows the 'Session' configuration page in VMware View. The 'Session Connection Type' is set to 'View Connection Server + Auto-Logon'. The 'DNS Name or IP Address' is 'viewdesktop.teradici.com'. The 'Desktop Name to Select' field is empty. The 'Port' is set to '(Leave blank for default)'. The 'VCS Certificate Check Mode' is 'Warn before connecting to untrusted servers'. The 'VCS Certificate Check Mode Lockout' checkbox is unchecked. The 'Trusted View Connection Servers' section has 'Show' and 'Clear' buttons. The 'Auto Connect' checkbox is unchecked. The 'Connection Server Cache Mode' is 'Last servers used' with a 'Clear cache entries' button. The 'Auto Launch If Only One Desktop' checkbox is checked. The 'Use OSD Logo for View banner' checkbox is unchecked. The 'Enable Peer Loss Overlay', 'Enable Preparing Desktop Overlay', and 'Enable Session Disconnect Hotkey' checkboxes are all unchecked. The 'Session Negotiation Cipher' is 'Maximum Compatibility: TLS 1.0 with RSA keys and AES-256 or AES-128 encryption'. The 'Enabled Session Ciphers' section shows 'AES-256-GCM' and 'AES-128-GCM' both checked. The 'Disconnect Message Filter' is 'Show All'. The 'Apply' and 'Cancel' buttons are at the bottom.

図 5-24 : AWI セッション接続タイプ – View Connection Server + 自動ログイン

表 5-30 : AWI Session ページパラメータ

パラメータ	説明
DNS Name or IP Address	VMware View Connection Server の DNS 名または IP アドレスを入力します。
Logon Username	クライアントのユーザ名を入力します。
Logon Password	クライアントのパスワードを入力します。
Logon Domain Name	クライアントのドメイン名を入力します。
Desktop Name to Select	セッションを開始するときにクライアントが使用するプールデスクトップ名を入力します。 注意：この設定は省略可能です。
Port	デフォルトで、このフィールドは空白になっており、View Connection Server との通信にはポート 443 が使用されます。ネットワークがセキュア接続用として非標準ポートを使用するようにセットアップされている場合は、ポート番号を入力します。
VCS Certificate Check Mode	クライアントが View Connection Server とのセキュア接続を確認できない場合の動作を選択します。 <ul style="list-style-type: none"> • Never connect to untrusted servers : 信頼できる有効な証明書がインストールされていない場合に接続を拒否するようにクライアントを設定します（これは最もセキュアなオプションです）。 • Warn before connecting to untrusted servers : 未署名のまたは期限切れの証明書を受信した場合、または、証明書が自己署名されておらず、ゼロクライアントのトラストストアが空の場合に警告を表示するようにクライアントを設定します（このオプションはデフォルトで選択されています）。 • Do not verify server identity certificates : すべての接続を許可するようにクライアントを設定します（このオプションはセキュアではありません）。
VCS Certificate Check Mode Lockout	ユーザが OSD から VCS Certificate Check Mode 設定を変更できないようにします。
Trusted View Connection Servers	Show ボタンをクリックすると、クライアントが有効な証明書を受信した VMware View Connection Server が表示されます。 Clear ボタンをクリックすると、このキャッシュがクリアされます。
Auto Connect	有効になっている場合は、クライアントが、電源がオンになっているときはいつでも、または、仮想デスクトップとのセッションが終了したときに、自動的に、選択された View Connection Server に接続し

パラメータ	説明
	<p>ます。</p> <p>注意： Auto Connect を有効にしたら、変更を反映させるためにクライアントの電源を入れ直す必要があります。</p>
Connection Server Cache Mode	<p>このフィールドは、ユーザが有効なサーバアドレスを入力したときに View Connection Server を OSD Connect ページの Server ドロップダウンメニューに動的に追加するかどうか、または、ユーザが選択するための読み取り専用リストに View Connection Server を表示するかどうかを決定します。</p> <ul style="list-style-type: none"> • Last servers used : ユーザが入力したキャッシュサーバのリストを OSD Connect ページの Server ドロップダウンメニューに表示したい場合にこのオプションを選択します。 • Read-only : ユーザに読み取り専用リストから View Connection Server を選択させたい場合にこのオプションを選択します。 <p>注意： PCoIP 管理コンソールを使用して、使用可能な接続サーバのリストを事前に生成しておくことができます。</p>
Enable Self Help Link	<p>詳細については、「セルフヘルプリンクの有効化」を参照してください。</p>
Auto Launch If Only One Desktop	<p>有効になっている場合は、ユーザ資格情報の入力後に、自動的に、ユーザが仮想デスクトップに接続されます。</p> <p>注意：この機能は、単一のデスクトップを使用可能なユーザにのみ適用されます。複数の仮想デスクトップを使用可能なユーザには適用されません。</p>
Login Username Caching	<p>有効になっている場合は、ユーザ名テキストボックスに、自動的に、最後に入力されたユーザ名が設定されます。</p>
Use OSD Logo for View Banner	<p>有効になっている場合は、ログイン中に、VMware View バナーの代わりに、PCoIP ゼロクライアント OSD ロゴが表示されます。OSD ロゴは OSD Logo Upload ページでアップロードすることができます。</p>
Prefer GSC-IS	<p>選択されている場合は、スマートカードで CAC (GSC-IS) や PIV エンドポイントなどの複数のインターフェースがサポートされていれば、GSC-IS インターフェースが使用されます。スマートカードで CAC と PIV エンドポイントのどちらかなどの 1 つのインターフェースしかサポートされていない場合は、この設定に関係なく、CAC または PIV エンドポイントインターフェースのみが使用されます。これは、PCoIP セッション以外で実行されるスマートカードアクセスにのみ影響を与えます。</p>
Enable Peer Loss Overlay	<p>有効になっている場合は、ネットワーク接続の消失が検出されたときに、“Network Connection Lost”オーバーレイがディスプレイ上に表示されます。このオーバーレイは VMware View などの仮想デスクトップ</p>

パラメータ	説明
	<p>プの場合にも表示されます。通常のハイパーバイザスケジューリングの遅延によってもこのメッセージが誤ってトリガーされる場合があります。</p> <p>注意：このオプションはゼロクライアントに対してしか使用することができません。ピア消失通知が必要なデスクトップアプリケーションは、OSD、AWI、またはMCを介してこの機能を再有効化する必要があります。</p>
<p>Enable Preparing Desktop Overlay</p>	<p>有効になっている場合は、ユーザがログインしたときに、"Preparing Desktop"オーバーレイがディスプレイ上に表示されます。</p> <p>注意：このオーバーレイは、デスクトップの表示に数秒以上かかっている場合でもログインが進行中であることを保証します。</p>
<p>Enable Session Disconnect Hotkey</p>	<p>有効になっている場合は、ユーザが Ctrl+Alt+F12 ホットキーシーケンスを押すと、"Zero Client Control Panel"オーバーレイがポップアップ表示されます。ここで、ユーザはワークステーション上の現在のセッションを切断したり、ワークステーションの電源をオフにしたりすることができます。</p> <p>注意：ユーザがこの切断ホットキーシーケンスを使用できるようにするには、他の特定の設定オプションを有効にする必要があります。詳細については、「セッションの切断」を参照してください。</p>
<p>Session Negotiation Cipher</p>	<p>クライアントが PCoIP クライアントと PCoIP ホスト間のトランスポート層セキュリティ (TLS) セッションをネゴシエートするために使用する TLS 暗号を設定します。</p> <ul style="list-style-type: none"> ● TLS 1.0 with RSA keys and AES-256 or AES-128 encryption : このオプションは最大限の互換性を提供します。 ● TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption : このオプションはより高度なセキュリティを提供します。
<p>Enabled Session Ciphers</p>	<p>デバイスの暗号化モードを有効または無効にします。デフォルトで、デバイスに関係するすべての暗号化モードが有効になっています。</p> <ul style="list-style-type: none"> ● AES-128-GCM (Tera1 と Tera2) : 第1世代 Tera1 プロセッサと第2世代 Tera2 プロセッサに実装されている暗号化方式。この方式では、Tera1 デバイスのハードウェアエンドポイント間で最高性能を実現することができます。また、Tera2 クライアントが VMware 4 以降に接続されており、ネットワーク上で 7 Mbps 以上の速度が利用可能であれば、高い性能を実現できる可能性があります。 ● AES-256-GCM (Tera2 のみ) : 第2世代 Tera2 プロセッサに実装されているよりセキュアな暗号化方式で、ハードウェアエンドポイント間で最高性能を実現することができます。VMware 4 以降に接続されている場合は、AES-128-GCM をお勧めします。 ● Salsa20-256-Round12 (Tera1 のみ) : Tera1 クライアントが VMware 4 以降に接続されており、ネットワーク上で 7 Mbps 以上

パラメータ	説明
	<p>の速度が利用可能であれば、高い性能を実現することが可能な、ファームウェアに実装されているより軽量の暗号化方式。</p> <p>注意：VMware View 仮想デスクトップへの接続方法については、『Using PCoIP Zero Clients with VMware View User Guide』（TER0904005）を参照してください。</p> <p>注意：有効にする暗号化モードは、セッションを確立するホストとクライアント間で一致させる必要があります。複数のモードが有効になっている場合は、ファームウェアが次のように選択します。</p> <ul style="list-style-type: none"> ● ホストと Tera1 または Tera2 クライアント間：PCoIP セッションに対して AES-128-GCM または AES-256-GCM ● VMware View 4.5 以降と Tera1 クライアント間：PCoIP セッションに対して SALSA20-256-Round12 ● VMware View 4.5 以降と Tera2 クライアント間：PCoIP セッションに対して AES-128-GCM
Disconnect Message Filter	<p>このフィールドを使用すれば、セッションが切断されたときに表示されるメッセージのタイプを制御することができます。次の 3 つのカテゴリに分かれています。</p> <p>情報：セッションに影響を与えるユーザまたは管理者によるアクション：</p> <ul style="list-style-type: none"> ● 別の場所からログインしたか、ホストがシャットダウンまたは再起動されたために切断されました。 ● 管理者が切断を実行したために切断されました。 ● 別の場所からログインしたために切断されました。 ● ワークステーションを切断したために切断されました。 <p>警告：セッションに影響を与えるシステムによる予想されるアクション：</p> <ul style="list-style-type: none"> ● セッションがタイムアウトしたために切断されました。 <p>エラー：セッションの失敗を引き起こす予期せぬシステムによるアクション：</p> <ul style="list-style-type: none"> ● 切断されました。 ● 接続できません (0x1001)。IT 管理者に連絡してください。 ● 接続できません (0x1002)。IT 管理者に連絡してください。 ● セッションがリモートで閉じられました。 ● セッションがリモートで閉じられました (原因不明)。 ● 設定エラーが原因で切断されました (0x100)。IT 管理者に支援を要請してください。 ● 設定エラーが原因で切断されました (0x201)。IT 管理者に支援を要請してください。 ● 設定エラーが原因で切断されました (0x300)。IT 管理者に支援を要請してください。 ● 設定エラーが原因で切断されました (0x301)。IT 管理者に支援を要請してください。 ● 設定エラーが原因で切断されました (0x302)。IT 管理者に支援

パラメータ	説明
	<p>を要請してください。</p> <ul style="list-style-type: none"> 設定エラーが原因で切断されました (0x303)。IT 管理者に支援を要請してください。 設定エラーが原因で切断されました (0x305)。IT 管理者に支援を要請してください。 設定エラーが原因で切断されました (0x400)。IT 管理者に支援を要請してください。 設定エラーが原因で切断されました (0x401)。IT 管理者に支援を要請してください。 設定エラーが原因で切断されました (0x402)。IT 管理者に支援を要請してください。 設定エラーが原因で切断されました (0x403)。IT 管理者に支援を要請してください。 設定エラーが原因で切断されました (0x404)。IT 管理者に支援を要請してください。 <p>以下の表示を選択することができます。</p> <ol style="list-style-type: none"> Show All messages – このオプションは、情報メッセージ、警告メッセージ、およびエラーメッセージを含むすべての切断メッセージを表示します。 Show Error and Warnings Only – このオプションは情報メッセージを表示せず、エラーメッセージと警告メッセージのみを表示します。 Show Error Only – このオプションは情報メッセージと警告メッセージを表示せず、エラーメッセージのみを表示します。 Show None – どの切断メッセージも表示しません。

セルフヘルプリンクの有効化

Self Help Link オプションを使用すれば、ユーザのセルフヘルプリンクを **Connect** ウィンドウに表示するように設定することができます。ログオン詳細を設定すると、ユーザがセルフヘルプリンクをクリックしたときに自動的に仮想マシンにログインすることが保証されます。

Enable Self Help Link:

View Connection Server:

Port: (Leave blank for default)

Username:

Password:

Domain:

Desktop Name to Select:

Link Text:

図 5-25 : Self Help Link オプションの有効化

このフィールドを有効にすると、次のようなオプションが表示されます。

パラメータ	説明
View Connection Server	セルフヘルプ仮想マシンをホストしている View Connection Server の名前を入力します。
Port	デフォルトで、このフィールドは空白になっており、View Connection Server との通信にはポート 443 が使用されます。ネットワークがセキュア接続用として非標準ポートを使用するようにセットアップされている場合は、ポート番号を入力します。
Username	セルフヘルプリンクに対して仮想マシンをパスワードで保護する場合に、このフィールドにユーザ名を入力します。
Password	セルフヘルプリンクに対して仮想マシンをパスワードで保護する場合に、このフィールドにパスワードを入力します。
Domain	セルフヘルプリンクの仮想マシンで使用されるドメイン名を入力します。
Desktop Name to Select	セルフヘルプリンクの仮想マシンで使用されるプールデスクトップ名を入力します。
Link Text	Connect ウィンドウにハイパーリンクとして表示するテキストを入力します。

5.6.14 AWI クライアント : View Connection Server + キオスクセッション設定

VMware View Connection Server を介して仮想デスクトップに接続するときにキオスクモードを使用するようにクライアントを設定する場合は、**Configuration > Session** ページで **View Connection Server + キオスクセッション** 接続タイプを選択します。

図 5-26 : AWI セッション接続タイプ – View Connection Server + キオスク

表 5-31 : AWI Session ページパラメータ

パラメータ	説明
DNS Name or IP Address	VMware View Connection Server の DNS 名または IP アドレスを入力します。
Username Type	View Connection Server 上でデバイスに使用するネーミングにマッチしたユーザ名のタイプを選択します。 <ul style="list-style-type: none"> • Zero Client MAC : このオプションは、自動的に、Username フィールドにゼロクライアントの MAC アドレスを設定する場合に選択します。 • Custom : ゼロクライアントのユーザ名を入力します。このユーザ名にはプレフィックスの"Custom"が付加されます。
Username	ユーザ名タイプとして Custom が選択されている場合に、このカスタムユーザ名要素の値を入力します。このフィールドは最大 13 文字に制限されています。

パラメータ	説明
Password	キオスクに対して仮想マシンをパスワードで保護する場合に、このフィールドにパスワードを入力します。このパスワードは、 View Connection Server でデバイスに対して入力されたものと同じにする必要があります。
Port	デフォルトで、このフィールドは空白になっており、 View Connection Server との通信にはポート 443 が使用されます。 ネットワークがセキュア接続用として非標準ポートを使用するようにセットアップされている場合は、ポート番号を入力します。
VCS Certificate Check Mode	クライアントが View Connection Server とのセキュア接続を確認できない場合の動作を選択します。 <ul style="list-style-type: none"> • Never connect to untrusted servers : 信頼できる有効な証明書がインストールされていない場合に接続を拒否するようにクライアントを設定します (これは最もセキュアなオプションです)。 • Warn before connecting to untrusted servers : 未署名のまたは期限切れの証明書を受信した場合、または、証明書が自己署名されておらず、ゼロクライアントのトラストストアが空の場合に警告を表示するようにクライアントを設定します (このオプションはデフォルトで選択されています)。 • Do not verify server identity certificates : すべての接続を許可するようにクライアントを設定します (このオプションはセキュアではありません)。
VCS Certificate Check Mode Lockout	ユーザが OSD から VCS Certificate Check Mode 設定を変更できないようにします。
Trusted View Connection Servers	Show ボタンをクリックすると、クライアントが有効な証明書を受信した VMware View Connection Server が表示されます。 Clear ボタンをクリックすると、このキャッシュがクリアされます。
Connection Server Cache Mode	このフィールドは、ユーザが有効なサーバアドレスを入力したときに View Connection Server を OSD Connect ページの Server ドロップダウンメニューに動的に追加するかどうか、または、ユーザが選択するための読み取り専用リストに View Connection Server を表示するかどうかを決定します。 <ul style="list-style-type: none"> • Last servers used : ユーザが入力したキャッシュサーバのリストを OSD Connect ページの Server ドロップダウンメニューに表示したい場合にこのオプションを選択します。 • Read-only : ユーザに読み取り専用リストから View Connection Server を選択させたい場合にこのオプションを選択します。 <p>注意 : PCoIP 管理コンソールを使用して、使用可能な接続サーバのリストを事前に生成しておくことができます。</p>
Use OSD Logo for View	有効になっている場合は、ログイン中に、VMware View バナーの代

パラメータ	説明
Banner	<p>代わりに、PCoIP ゼロクライアント OSD ロゴが表示されます。OSD ロゴは OSD Logo Upload ページでアップロードすることができます。</p>
Enable Peer Loss Overlay	<p>有効になっている場合は、ネットワーク接続の消失が検出されたときに、“Network Connection Lost”オーバーレイがディスプレイ上に表示されます。このオーバーレイは VMware View などの仮想デスクトップの場合にも表示されます。通常のハイパーバイザスケジューリングの遅延によってもこのメッセージが誤ってトリガーされる場合があります。</p> <p>注意：このオプションはゼロクライアントに対してしか使用することができません。ピア消失通知が必要なデスクトップアプリケーションは、OSD、AWI、または MC を介してこの機能を再有効化する必要があります。</p>
Enable Preparing Desktop Overlay	<p>有効になっている場合は、ユーザがログインしたときに、“Preparing Desktop”オーバーレイがディスプレイ上に表示されます。</p> <p>注意：このオーバーレイは、デスクトップの表示に数秒以上かかっている場合でもログインが進行中であることを保証します。</p>
Enable Session Disconnect Hotkey	<p>有効になっている場合は、ユーザが Ctrl+Alt+F12 ホットキーシーケンスを押すと、“Zero Client Control Panel”オーバーレイがポップアップ表示されます。ここで、ユーザはワークステーション上の現在のセッションを切断したり、ワークステーションの電源をオフにしたりすることができます。</p> <p>注意：ユーザがこの切断ホットキーシーケンスを使用できるようにするには、他の特定の設定オプションを有効にする必要があります。詳細については、「セッションの切断」を参照してください。</p>
Session Negotiation Cipher	<p>クライアントが PCoIP クライアントと PCoIP ホスト間のトランスポート層セキュリティ (TLS) セッションをネゴシエートするために使用する TLS 暗号を設定します。</p> <ul style="list-style-type: none"> • TLS 1.0 with RSA keys and AES-256 or AES-128 encryption : このオプションは最大限の互換性を提供します。 • TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption : このオプションはより高度なセキュリティを提供します。
Enabled Session Ciphers	<p>デバイスの暗号化モードを有効または無効にします。デフォルトで、デバイスに関係するすべての暗号化モードが有効になっています。</p> <ul style="list-style-type: none"> • AES-128-GCM (Tera1 と Tera2) : 第 1 世代 Tera1 プロセッサと第 2 世代 Tera2 プロセッサに実装されている暗号化方式。この方式では、Tera1 デバイスのハードウェアエンドポイント間で最高性能を実現することができます。また、Tera2 クライアントが VMware 4 以降に接続されており、ネットワーク上で 7 Mbps 以上の速度が利用可能であれば、高い性能を実現できる可能性があります。

パラメータ	説明
	<ul style="list-style-type: none"> • AES-256-GCM (Tera2 のみ) : 第 2 世代 Tera2 プロセッサに実装されているよりセキュアな暗号化方式で、ハードウェアエンドポイント間で最高性能を実現することができます。VMware 4 以降に接続されている場合は、AES-128-GCM をお勧めします。 • Salsa20-256-Round12 (Tera1 のみ) : Tera1 クライアントが VMware 4 以降に接続されており、ネットワーク上で 7 Mbps 以上の速度が利用可能であれば、高い性能を実現することが可能な、ファームウェアに実装されているより軽量の暗号化方式。 <p>注意 : VMware View 仮想デスクトップへの接続方法については、『Using PCoIP Zero Clients with VMware View User Guide』(TER0904005) を参照してください。</p> <p>注意 : 有効にする暗号化モードは、セッションを確立するホストとクライアント間で一致させる必要があります。複数のモードが有効になっている場合は、ファームウェアが次のように選択します。</p> <ul style="list-style-type: none"> • ホストと Tera1 または Tera2 クライアント間 : PCoIP セッションに対して AES-128-GCM または AES-256-GCM • VMware View 4.5 以降と Tera1 クライアント間 : PCoIP セッションに対して SALSA20-256-Round12 • VMware View 4.5 以降と Tera2 クライアント間 : PCoIP セッションに対して AES-128-GCM
Disconnect Message Filter	<p>このフィールドを使用すれば、セッションが切断されたときに表示されるメッセージのタイプを制御することができます。次の 3 つのカテゴリに分かれています。</p> <p>情報 : セッションに影響を与えるユーザまたは管理者によるアクション :</p> <ul style="list-style-type: none"> • 別の場所からログインしたか、ホストがシャットダウンまたは再起動されたために切断されました。 • 管理者が切断を実行したために切断されました。 • 別の場所からログインしたために切断されました。 • ワークステーションを切断したために切断されました。 <p>警告 : セッションに影響を与えるシステムによる予想されるアクション :</p> <ul style="list-style-type: none"> • セッションがタイムアウトしたために切断されました。 <p>エラー : セッションの失敗を引き起こす予期せぬシステムによるアクション :</p> <ul style="list-style-type: none"> • 切断されました。 • 接続できません (0x1001) 。 IT 管理者に連絡してください。 • 接続できません (0x1002) 。 IT 管理者に連絡してください。 • セッションがリモートで閉じられました。 • セッションがリモートで閉じられました (原因不明) 。 • 設定エラーが原因で切断されました (0x100) 。 IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x201) 。 IT 管理者に支援

パラメータ	説明
	<p>を要請してください。</p> <ul style="list-style-type: none"> • 設定エラーが原因で切断されました (0x300)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x301)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x302)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x303)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x305)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x400)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x401)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x402)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x403)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x404)。IT 管理者に支援を要請してください。 <p>以下の表示を選択することができます。</p> <ol style="list-style-type: none"> 1. Show All messages – このオプションは、情報メッセージ、警告メッセージ、およびエラーメッセージを含むすべての切断メッセージを表示します。 2. Show Error and Warnings Only – このオプションは情報メッセージを表示せず、エラーメッセージと警告メッセージのみを表示します。 3. Show Error Only – このオプションは情報メッセージと警告メッセージを表示せず、エラーメッセージのみを表示します。 4. Show None – どの切断メッセージも表示しません。

5.6.15 AWI クライアント : View Connection Server + Imprivata OneSign セッション設定

仮想デスクトップに接続するときに View Connection Server に加えて Imprivata OneSign システム経由でも認証するようにクライアントを設定する場合は、**Configuration > Session** ページで **View Connection Server + Imprivata OneSign** セッション接続タイプを選択します。

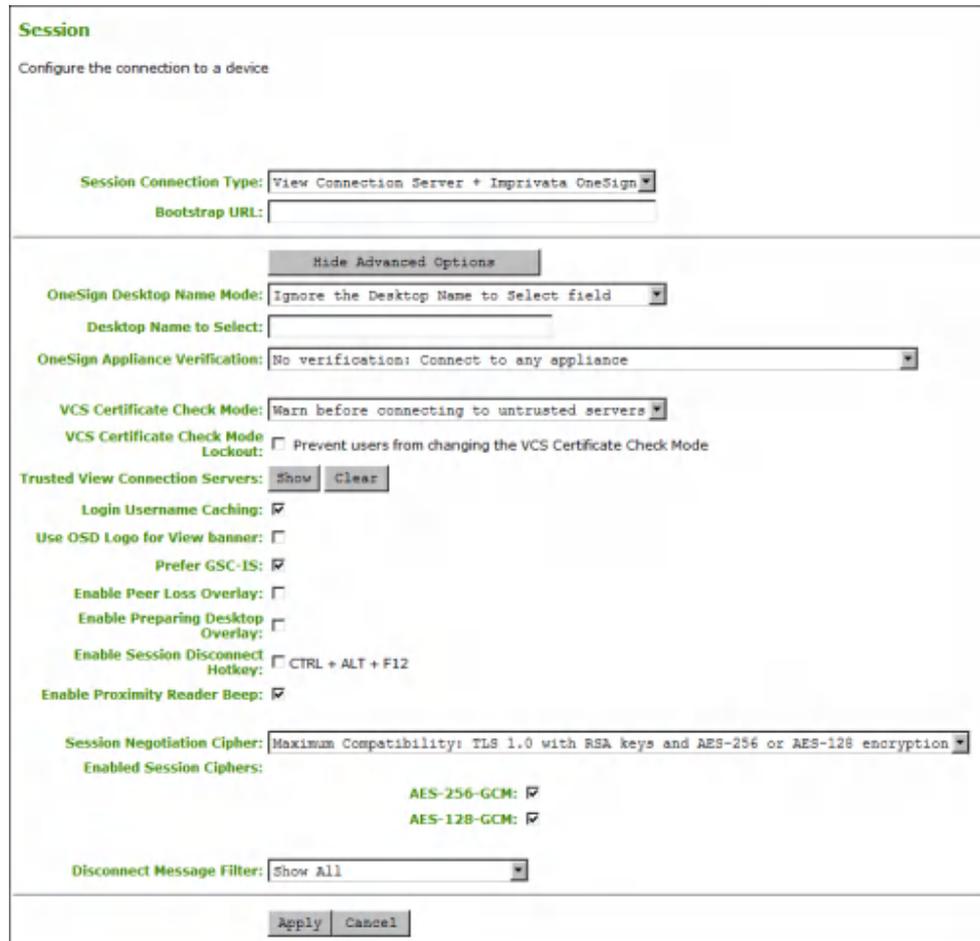


図 5-27 : AWI セッション接続タイプ – View Connection Server + Imprivata OneSign

表 5-32 : AWI Session ページパラメータ

パラメータ	説明
DNS Name or IP Address	VMware View Connection Server の DNS 名または IP アドレスを入力します。
Bootstrap URL	OneSign 認証デプロイメント内で初期 OneSign サーバを探すために使用されるブートストラップ URL を入力します。
Onesign Desktop Name Mode	Desktop Name to Select プロパティが OneSign モードで使用されるかどうかを選択します。 <ul style="list-style-type: none"> • Ignore • Use If Set
Desktop Name to Select	デスクトップ名を入力します。デスクトッププールリストにこの名前のプールが含まれている場合は、クライアントが即座にそのプールを

パラメータ	説明
	使用したセッションを開始します。 注意：このフィールドは大文字と小文字が区別されます。
Onesign Appliance Verification	OneSign アプライアンスサーバから提示された証明書に対して実施される検証のレベルを設定します。 <ul style="list-style-type: none"> • No verification：任意のアプライアンスに接続します。 • Full verification：証明書が検証済みのアプライアンスにのみ接続します。
VCS Certificate Check Mode	クライアントが View Connection Server とのセキュア接続を確認できない場合の動作を選択します。 <ul style="list-style-type: none"> • Never connect to untrusted servers：信頼できる有効な証明書がインストールされていない場合に接続を拒否するようにクライアントを設定します（これは最もセキュアなオプションです）。 • Warn before connecting to untrusted servers：未署名のまたは期限切れの証明書を受信した場合、または、証明書が自己署名されておらず、ゼロクライアントのトラストストアが空の場合に警告を表示するようにクライアントを設定します（このオプションはデフォルトで選択されています）。 • Do not verify server identity certificates：すべての接続を許可するようにクライアントを設定します（このオプションはセキュアではありません）。
VCS Certificate Check Mode Lockout	ユーザが OSD から VCS Certificate Check Mode 設定を変更できないようにします。
Trusted View Connection Servers	Show ボタンをクリックすると、クライアントが有効な証明書を受信した VMware View Connection Server が表示されます。 Clear ボタンをクリックすると、このキャッシュがクリアされます。
Login Username Caching	有効になっている場合は、ユーザ名テキストボックスに、自動的に、最後に入力されたユーザ名が設定されます。
Use OSD Logo for View Banner	有効になっている場合は、ログイン中に、VMware View バナーの代わりに、PCoIP ゼロクライアント OSD ロゴが表示されます。OSD ロゴは OSD Logo Upload ページでアップロードすることができます。
Prefer GSC-IS	選択されている場合は、スマートカードで CAC (GSC-IS) や PIV エンドポイントなどの複数のインターフェースがサポートされていれば、GSC-IS インターフェースが使用されます。スマートカードで CAC と PIV エンドポイントのどちらかなどの 1 つのインターフェースしかサポートされていない場合は、この設定に関係なく、CAC または PIV エンドポイントインターフェースのみが使用されます。これは、PCoIP セッション以外で実行されるスマートカードアクセスのみ影響を与えます。

パラメータ	説明
Enable Peer Loss Overlay	<p>有効になっている場合は、ネットワーク接続の消失が検出されたときに、“Network Connection Lost”オーバーレイがディスプレイ上に表示されます。このオーバーレイは VMware View などの仮想デスクトップの場合にも表示されます。通常のハイパーバイザスケジューリングの遅延によってもこのメッセージが誤ってトリガーされる場合があります。</p> <p>注意：このオプションはゼロクライアントに対してしか使用することができません。ピア消失通知が必要なデスクトップアプリケーションは、OSD、AWI、または MC を介してこの機能を再有効化する必要があります。</p>
Enable Preparing Desktop Overlay	<p>有効になっている場合は、ユーザがログインしたときに、“Preparing Desktop”オーバーレイがディスプレイ上に表示されます。</p> <p>注意：このオーバーレイは、デスクトップの表示に数秒以上かかっている場合でもログインが進行中であることを保証します。</p>
Enable Session Disconnect Hotkey	<p>有効になっている場合は、ユーザが Ctrl+Alt+F12 ホットキーシーケンスを押すと、“Zero Client Control Panel”オーバーレイがポップアップ表示されます。ここで、ユーザはワークステーション上の現在のセッションを切断したり、ワークステーションの電源をオフにしたりすることができます。</p> <p>注意：ユーザがこの切断ホットキーシーケンスを使用できるようにするには、他の特定の設定オプションを有効にする必要があります。詳細については、「セッションの切断」を参照してください。</p>
Session Negotiation Cipher	<p>クライアントが PCoIP クライアントと PCoIP ホスト間のトランスポート層セキュリティ (TLS) セッションをネゴシエートするために使用する TLS 暗号を設定します。</p> <ul style="list-style-type: none"> • TLS 1.0 with RSA keys and AES-256 or AES-128 encryption : このオプションは最大限の互換性を提供します。 • TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption : このオプションはより高度なセキュリティを提供します。
Enabled Session Ciphers	<p>デバイスの暗号化モードを有効または無効にします。デフォルトで、デバイスに関係するすべての暗号化モードが有効になっています。</p> <ul style="list-style-type: none"> • AES-128-GCM (Tera1 と Tera2) : 第 1 世代 Tera1 プロセッサと第 2 世代 Tera2 プロセッサに実装されている暗号化方式。この方式では、Tera1 デバイスのハードウェアエンドポイント間で最高性能を実現することができます。また、Tera2 クライアントが VMware 4 以降に接続されており、ネットワーク上で 7 Mbps 以上の速度が利用可能であれば、高い性能を実現できる可能性があります。 • AES-256-GCM (Tera2 のみ) : 第 2 世代 Tera2 プロセッサに実装されているよりセキュアな暗号化方式で、ハードウェアエンドポイント間で最高性能を実現することができます。VMware 4 以

パラメータ	説明
	<p>降に接続されている場合は、AES-128-GCMをお勧めします。</p> <ul style="list-style-type: none"> ● Salsa20-256-Round12 (Tera1のみ) : Tera1クライアントがVMware 4以降に接続されており、ネットワーク上で7 Mbps以上の速度が利用可能であれば、高い性能を実現することが可能な、ファームウェアに実装されているより軽量の暗号化方式。 <p>注意：VMware View 仮想デスクトップへの接続方法については、『Using PCoIP Zero Clients with VMware View User Guide』(TER0904005)を参照してください。</p> <p>注意：有効にする暗号化モードは、セッションを確立するホストとクライアント間で一致させる必要があります。複数のモードが有効になっている場合は、ファームウェアが次のように選択します。</p> <ul style="list-style-type: none"> ● ホストと Tera1 または Tera2 クライアント間：PCoIPセッションに対して AES-128-GCM または AES-256-GCM ● VMware View 4.5 以降と Tera1 クライアント間：PCoIPセッションに対して SALS20-256-Round12 ● VMware View 4.5 以降と Tera2 クライアント間：PCoIPセッションに対して AES-128-GCM
Disconnect Message Filter	<p>このフィールドを使用すれば、セッションが切断されたときに表示されるメッセージのタイプを制御することができます。次の3つのカテゴリに分かれています。</p> <p>情報：セッションに影響を与えるユーザまたは管理者によるアクション：</p> <ul style="list-style-type: none"> ● 別の場所からログインしたか、ホストがシャットダウンまたは再起動されたために切断されました。 ● 管理者が切断を実行したために切断されました。 ● 別の場所からログインしたために切断されました。 ● ワークステーションを切断したために切断されました。 <p>警告：セッションに影響を与えるシステムによる予想されるアクション：</p> <ul style="list-style-type: none"> ● セッションがタイムアウトしたために切断されました。 <p>エラー：セッションの失敗を引き起こす予期せぬシステムによるアクション：</p> <ul style="list-style-type: none"> ● 切断されました。 ● 接続できません (0x1001)。IT管理者に連絡してください。 ● 接続できません (0x1002)。IT管理者に連絡してください。 ● セッションがリモートで閉じられました。 ● セッションがリモートで閉じられました (原因不明)。 ● 設定エラーが原因で切断されました (0x100)。IT管理者に支援を要請してください。 ● 設定エラーが原因で切断されました (0x201)。IT管理者に支援を要請してください。 ● 設定エラーが原因で切断されました (0x300)。IT管理者に支援を要請してください。

パラメータ	説明
	<ul style="list-style-type: none"> • 設定エラーが原因で切断されました (0x301)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x302)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x303)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x305)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x400)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x401)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x402)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x403)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x404)。IT 管理者に支援を要請してください。 <p>以下の表示を選択することができます。</p> <ol style="list-style-type: none"> 1. Show All messages – このオプションは、情報メッセージ、警告メッセージ、およびエラーメッセージを含むすべての切断メッセージを表示します。 2. Show Error and Warnings Only – このオプションは情報メッセージを表示せず、エラーメッセージと警告メッセージのみを表示します。 3. Show Error Only – このオプションは情報メッセージと警告メッセージを表示せず、エラーメッセージのみを表示します。 4. Show None – どの切断メッセージも表示しません。

5.6.16 AWI ホスト : Connection Management Interface セッション設定

外部コネクションマネージャをホストが使用する [コネクションブローカ](#) として設定する場合は、**Configuration > Session** ページで **Connection Management Interface** セッション接続タイプを選択します。

注意：外部コネクションマネージャは大規模で複雑なシステムの管理手順を簡略化することができます。管理接続では、外部コネクションマネージャサーバがデバイスと通信して、それをリモートで制御および設定することができます。コネクションマネージャは、接続するデバイスに適切なピアを特定してから接続を開始することもできます。

図 5-28 : AWI セッション接続タイプ – Connection Management Interface (ホスト)

表 5-33 : AWI Session ページパラメータ

パラメータ	説明
DNS Name or IP Address	コネクションマネージャの DNS 名または IP アドレスを入力します。
Session Negotiation Cipher	<p>クライアントが PCoIP クライアントと PCoIP ホスト間のトランスポート層セキュリティ (TLS) セッションをネゴシエートするために使用する TLS 暗号を設定します。</p> <ul style="list-style-type: none"> • TLS 1.0 with RSA keys and AES-256 or AES-128 encryption : このオプションは最大限の互換性を提供します。 • TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption : このオプションはより高度なセキュリティを提供します。
Enabled Session Ciphers	<p>デバイスの暗号化モードを有効または無効にします。デフォルトで、デバイスに関係するすべての暗号化モードが有効になっています。</p> <ul style="list-style-type: none"> • AES-128-GCM (Tera1 と Tera2) : 第 1 世代 Tera1 プロセッサと第 2 世代 Tera2 プロセッサに実装されている暗号化方式。この方式では、Tera1 デバイスのハードウェアエンドポイント間で最高性能を実現することができます。また、Tera2 クライアントが VMware 4 以降に接続されており、ネットワーク上で 7 Mbps 以上の速度が利用可能であれば、高い性能を実現できる可能性があります。 • AES-256-GCM (Tera2 のみ) : 第 2 世代 Tera2 プロセッサに実装されているよりセキュアな暗号化方式で、ハードウェアエンドポイント間で最高性能を実現することができます。VMware 4 以降に接続されている場合は、AES-128-GCM をお勧めします。 • Salsa20-256-Round12 (Tera1 のみ) : Tera1 クライアントが VMware 4 以降に接続されており、ネットワーク上で 7 Mbps 以上の速度が利用可能であれば、高い性能を実現することが可能な、ファームウェアに実装されているより軽量な暗号化方式。

パラメータ	説明
	<p>注意：VMware View 仮想デスクトップへの接続方法については、『Using PCoIP Zero Clients with VMware View User Guide』（TER0904005）を参照してください。</p> <p>注意：有効にする暗号化モードは、セッションを確立するホストとクライアント間で一致させる必要があります。複数のモードが有効になっている場合は、ファームウェアが次のように選択します。</p> <ul style="list-style-type: none"> ● ホストと Tera1 または Tera2 クライアント間：PCoIP セッションに対して AES-128-GCM または AES-256-GCM ● VMware View 4.5 以降と Tera1 クライアント間：PCoIP セッションに対して SALSA20-256-Round12 ● VMware View 4.5 以降と Tera2 クライアント間：PCoIP セッションに対して AES-128-GCM
Disconnect Message Filter	<p>このフィールドを使用すれば、セッションが切断されたときに表示されるメッセージのタイプを制御することができます。次の 3 つのカテゴリに分かれています。</p> <p>情報：セッションに影響を与えるユーザまたは管理者によるアクション：</p> <ul style="list-style-type: none"> ● 別の場所からログインしたか、ホストがシャットダウンまたは再起動されたために切断されました。 ● 管理者が切断を実行したために切断されました。 ● 別の場所からログインしたために切断されました。 ● ワークステーションを切断したために切断されました。 <p>警告：セッションに影響を与えるシステムによる予想されるアクション：</p> <ul style="list-style-type: none"> ● セッションがタイムアウトしたために切断されました。 <p>エラー：セッションの失敗を引き起こす予期せぬシステムによるアクション：</p> <ul style="list-style-type: none"> ● 切断されました。 ● 接続できません (0x1001)。IT 管理者に連絡してください。 ● 接続できません (0x1002)。IT 管理者に連絡してください。 ● セッションがリモートで閉じられました。 ● セッションがリモートで閉じられました (原因不明)。 ● 設定エラーが原因で切断されました (0x100)。IT 管理者に支援を要請してください。 ● 設定エラーが原因で切断されました (0x201)。IT 管理者に支援を要請してください。 ● 設定エラーが原因で切断されました (0x300)。IT 管理者に支援を要請してください。 ● 設定エラーが原因で切断されました (0x301)。IT 管理者に支援を要請してください。 ● 設定エラーが原因で切断されました (0x302)。IT 管理者に支援を要請してください。 ● 設定エラーが原因で切断されました (0x303)。IT 管理者に支援

パラメータ	説明
	<p>を要請してください。</p> <ul style="list-style-type: none"> • 設定エラーが原因で切断されました (0x305)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x400)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x401)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x402)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x403)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x404)。IT 管理者に支援を要請してください。 <p>以下の表示を選択することができます。</p> <ol style="list-style-type: none"> 1. Show All messages – このオプションは、情報メッセージ、警告メッセージ、およびエラーメッセージを含むすべての切断メッセージを表示します。 2. Show Error and Warnings Only – このオプションは情報メッセージを表示せず、エラーメッセージと警告メッセージのみを表示します。 3. Show Error Only – このオプションは情報メッセージと警告メッセージを表示せず、エラーメッセージのみを表示します。 4. Show None – どの切断メッセージも表示しません。

5.6.17 AWI クライアント : Connection Management Interface セッション設定

VMware View Connection Server 以外の外部接続マネージャをクライアントが使用する [コネクションブローカ](#) として設定する場合は、**Configuration > Session** ページで **Connection Management Interface** セッション接続タイプを選択します。

注意：外部接続マネージャは大規模で複雑なシステムの管理手順を簡略化することができます。管理接続では、外部接続マネージャサーバがデバイスと通信して、それをリモートで制御および設定することができます。コネクションマネージャは、接続するデバイスに適切なピアを特定してから接続を開始することもできます。

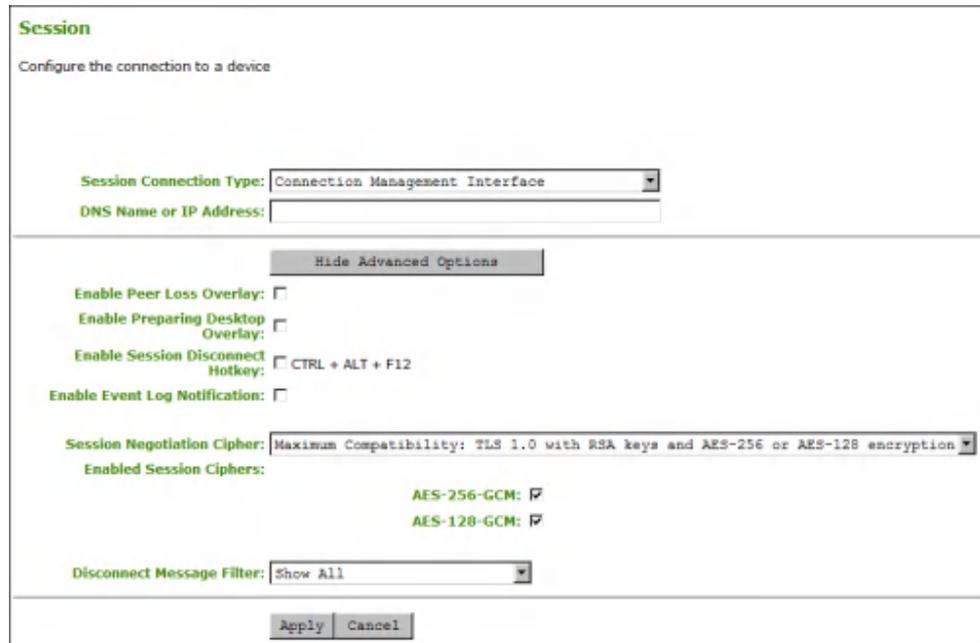


図 5-29 : AWI セッション接続タイプ – Connection Management Interface (クライアント)

表 5-34 : AWI Session ページパラメータ

パラメータ	説明
DNS Name or IP Address	コネクションマネージャの DNS 名または IP アドレスを入力します。
Enable Peer Loss Overlay	有効になっている場合は、ネットワーク接続の消失が検出されたときに、“Network Connection Lost”オーバーレイがディスプレイ上に表示されます。このオーバーレイは VMware View などの仮想デスクトップの場合にも表示されます。通常のハイパーバイザスケジューリングの遅延によってもこのメッセージが誤ってトリガーされる場合があります。 注意：このオプションはゼロクライアントに対してしか使用することができません。ピア消失通知が必要なデスクトップアプリケーションは、OSD、AWI、または MC を介してこの機能を再有効化する必要があります。
Enable Preparing Desktop Overlay	有効になっている場合は、ユーザがログインしたときに、“Preparing Desktop”オーバーレイがディスプレイ上に表示されます。 注意：このオーバーレイは、デスクトップの表示に数秒以上かかっている場合でもログインが進行中であることを保証します。
Enable Session Disconnect Hotkey	有効になっている場合は、ユーザが Ctrl+Alt+F12 ホットキーシーケンスを押すと、“Zero Client Control Panel”オーバーレイがポップアップ表示されます。ここで、ユーザはワークステーション上の現在のセッ

パラメータ	説明
	<p>セッションを切断したり、ワークステーションの電源をオフにしたりすることができます。</p> <p>注意：ユーザがこの切断ホットキーシーケンスを使用できるようにするには、他の特定の設定オプションを有効にする必要があります。詳細については、「セッションの切断」を参照してください。</p>
Enable Event Log Notification	<p>有効になっている場合は、クライアントがそのイベントログの内容を接続管理サーバに送信します。</p>
Session Negotiation Cipher	<p>クライアントが PCoIP クライアントと PCoIP ホスト間のトランスポート層セキュリティ (TLS) セッションをネゴシエートするために使用する TLS 暗号を設定します。</p> <ul style="list-style-type: none"> • TLS 1.0 with RSA keys and AES-256 or AES-128 encryption : このオプションは最大限の互換性を提供します。 • TLS 1.2 with Suite B-compliant 192-bit elliptic curve encryption : このオプションはより高度なセキュリティを提供します。
Enabled Session Ciphers	<p>デバイスの暗号化モードを有効または無効にします。デフォルトで、デバイスに関するすべての暗号化モードが有効になっています。</p> <ul style="list-style-type: none"> • AES-128-GCM (Tera1 と Tera2) : 第 1 世代 Tera1 プロセッサと第 2 世代 Tera2 プロセッサに実装されている暗号化方式。この方式では、Tera1 デバイスのハードウェアエンドポイント間で最高性能を実現することができます。また、Tera2 クライアントが VMware 4 以降に接続されており、ネットワーク上で 7 Mbps 以上の速度が利用可能であれば、高い性能を実現できる可能性があります。 • AES-256-GCM (Tera2 のみ) : 第 2 世代 Tera2 プロセッサに実装されているよりセキュアな暗号化方式で、ハードウェアエンドポイント間で最高性能を実現することができます。VMware 4 以降に接続されている場合は、AES-128-GCM をお勧めします。 • Salsa20-256-Round12 (Tera1 のみ) : Tera1 クライアントが VMware 4 以降に接続されており、ネットワーク上で 7 Mbps 以上の速度が利用可能であれば、高い性能を実現することが可能な、ファームウェアに実装されているより軽量の暗号化方式。 <p>注意：VMware View 仮想デスクトップへの接続方法については、『Using PCoIP Zero Clients with VMware View User Guide』(TER0904005) を参照してください。</p> <p>注意：有効にする暗号化モードは、セッションを確立するホストとクライアント間で一致させる必要があります。複数のモードが有効になっている場合は、ファームウェアが次のように選択します。</p> <ul style="list-style-type: none"> • ホストと Tera1 または Tera2 クライアント間：PCoIP セッションに対して AES-128-GCM または AES-256-GCM • VMware View 4.5 以降と Tera1 クライアント間：PCoIP セッションに対して SALS20-256-Round12 • VMware View 4.5 以降と Tera2 クライアント間：PCoIP セッション

パラメータ	説明
	ンに対して AES-128-GCM
Disconnect Message Filter	<p>このフィールドを使用すれば、セッションが切断されたときに表示されるメッセージのタイプを制御することができます。次の3つのカテゴリに分かれています。</p> <p>情報：セッションに影響を与えるユーザまたは管理者によるアクション：</p> <ul style="list-style-type: none"> • 別の場所からログインしたか、ホストがシャットダウンまたは再起動されたために切断されました。 • 管理者が切断を実行したために切断されました。 • 別の場所からログインしたために切断されました。 • ワークステーションを切断したために切断されました。 <p>警告：セッションに影響を与えるシステムによる予想されるアクション：</p> <ul style="list-style-type: none"> • セッションがタイムアウトしたために切断されました。 <p>エラー：セッションの失敗を引き起こす予期せぬシステムによるアクション：</p> <ul style="list-style-type: none"> • 切断されました。 • 接続できません (0x1001)。IT 管理者に連絡してください。 • 接続できません (0x1002)。IT 管理者に連絡してください。 • セッションがリモートで閉じられました。 • セッションがリモートで閉じられました (原因不明)。 • 設定エラーが原因で切断されました (0x100)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x201)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x300)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x301)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x302)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x303)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x305)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x400)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x401)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x402)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x403)。IT 管理者に支援を要請してください。

パラメータ	説明
	<ul style="list-style-type: none"> 設定エラーが原因で切断されました (0x404) 。IT 管理者に支援を要請してください。 <p>以下の表示を選択することができます。</p> <ol style="list-style-type: none"> Show All messages – このオプションは、情報メッセージ、警告メッセージ、およびエラーメッセージを含むすべての切断メッセージを表示します。 Show Error and Warnings Only – このオプションは情報メッセージを表示せず、エラーメッセージと警告メッセージのみを表示します。 Show Error Only – このオプションは情報メッセージと警告メッセージを表示せず、エラーメッセージのみを表示します。 Show None – どの切断メッセージも表示しません。

5.6.18 OSD : Direct to Host セッション設定

ホストに直接接続するようにクライアントを設定する場合は、**Options > Configuration > Session** ページで **Direct to Host** セッション接続タイプを選択します。このオプションの詳細設定を構成するには、**Advanced** ボタンをクリックします。

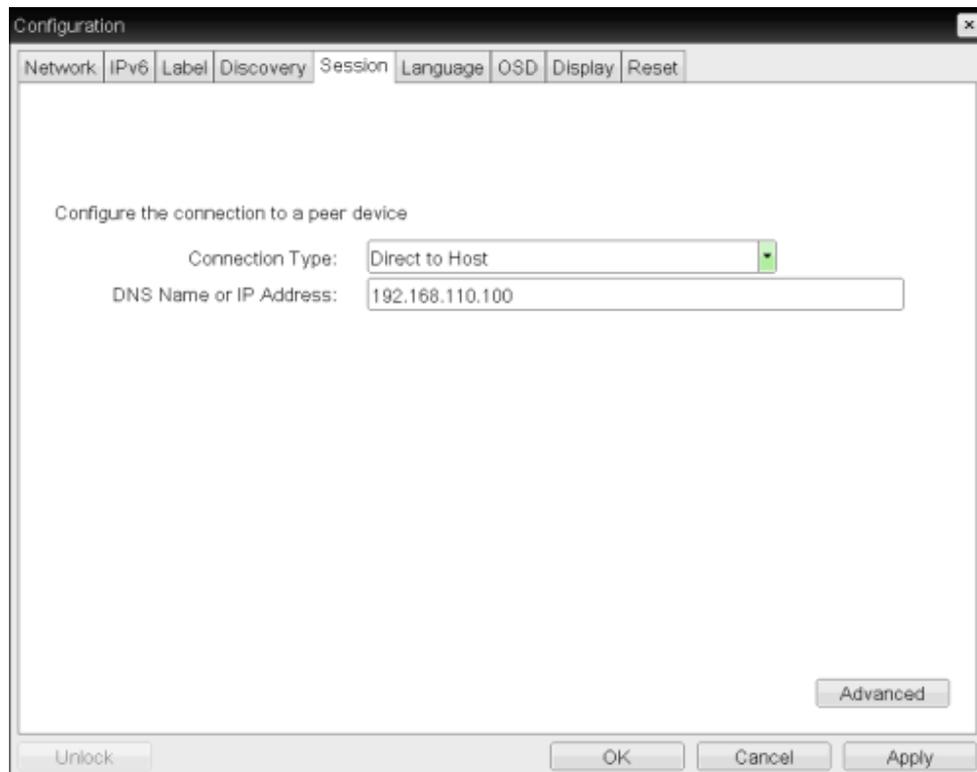


図 5-30 : OSD セッション接続タイプ – Direct to Host

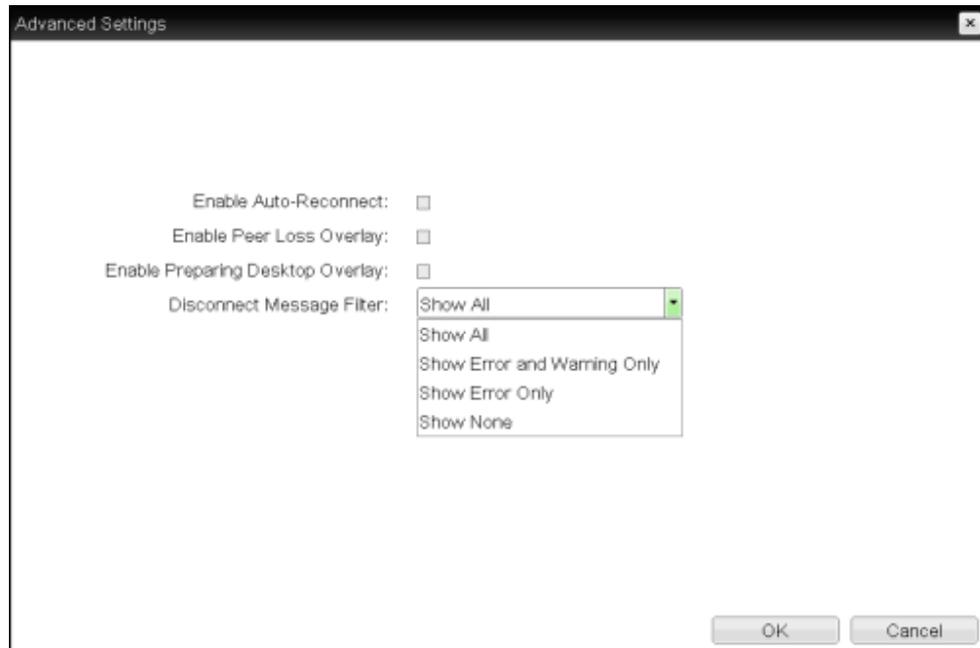


図 5-31 : Advanced Settings

表 5-35 : OSD Session ページパラメータ

パラメータ	説明
DNS Name or IP Address	ホストの IP アドレスまたは DNS 名を入力します。
Enable Auto-Reconnect	有効になっている場合は、セッションが失われたときに、クライアントが自動的に最後に接続していたホストに再接続します。
Enable Peer Loss Overlay	<p>有効になっている場合は、ネットワーク接続の消失が検出されたときに、“Network Connection Lost”オーバーレイがディスプレイ上に表示されます。このオーバーレイは VMware View などの仮想デスクトップの場合にも表示されます。通常のハイパーバイザスケジューリングの遅延によってもこのメッセージが誤ってトリガーされる場合があります。</p> <p>注意：このオプションはゼロクライアントに対してしか使用することができません。ピア消失通知が必要なデスクトップアプリケーションは、OSD、AWI、または MC を介してこの機能を再有効化する必要があります。</p>
Enable Preparing Desktop Overlay	<p>有効になっている場合は、ユーザがログインしたときに、“Preparing Desktop”オーバーレイがディスプレイ上に表示されます。</p> <p>注意：このオーバーレイは、デスクトップの表示に数秒以上かかっている場合でもログインが進行中であることを保証します。</p>

パラメータ	説明
Disconnect Message Filter	<p>このフィールドを使用すれば、セッションが切断されたときに表示されるメッセージのタイプを制御することができます。次の3つのカテゴリに分かれています。</p> <p>情報：セッションに影響を与えるユーザまたは管理者によるアクション：</p> <ul style="list-style-type: none"> • 別の場所からログインしたか、ホストがシャットダウンまたは再起動されたために切断されました。 • 管理者が切断を実行したために切断されました。 • 別の場所からログインしたために切断されました。 • ワークステーションを切断したために切断されました。 <p>警告：セッションに影響を与えるシステムによる予想されるアクション：</p> <ul style="list-style-type: none"> • セッションがタイムアウトしたために切断されました。 <p>エラー：セッションの失敗を引き起こす予期せぬシステムによるアクション：</p> <ul style="list-style-type: none"> • 切断されました。 • 接続できません (0x1001)。IT 管理者に連絡してください。 • 接続できません (0x1002)。IT 管理者に連絡してください。 • セッションがリモートで閉じられました。 • セッションがリモートで閉じられました (原因不明)。 • 設定エラーが原因で切断されました (0x100)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x201)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x300)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x301)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x302)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x303)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x305)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x400)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x401)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x402)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x403)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x404)。IT 管理者に支援を要請してください。

パラメータ	説明
	以下の表示を選択することができます。 <ol style="list-style-type: none"> 1. Show All messages – このオプションは、情報メッセージ、警告メッセージ、およびエラーメッセージを含むすべての切断メッセージを表示します。 2. Show Error and Warnings Only – このオプションは情報メッセージを表示せず、エラーメッセージと警告メッセージのみを表示します。 3. Show Error Only – このオプションは情報メッセージと警告メッセージを表示せず、エラーメッセージのみを表示します。 4. Show None – どの切断メッセージも表示しません。

5.6.19 OSD : Direct to Host + SLP ホストディスカバリセッション設定

ホストに直接接続したり、サービスローケーションプロトコル (SLP) 経由で自動的にホストを発見したりするようにクライアントを設定する場合は、**Options > Configuration > Session** ページで **Direct to Host + SLP ホストディスカバリセッション** 接続タイプを選択します。

このオプションの詳細設定を構成するには、**Advanced** ボタンをクリックします。

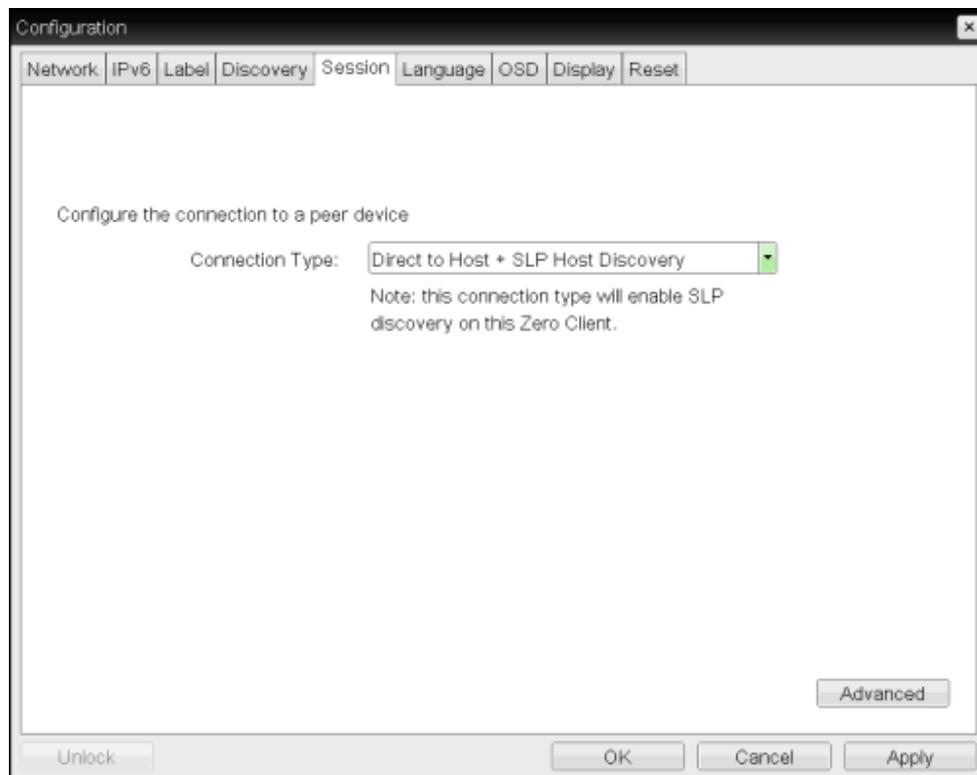


図 5-32 : OSD セッション接続タイプ – Direct to Host + SLP ホストディスカバリ

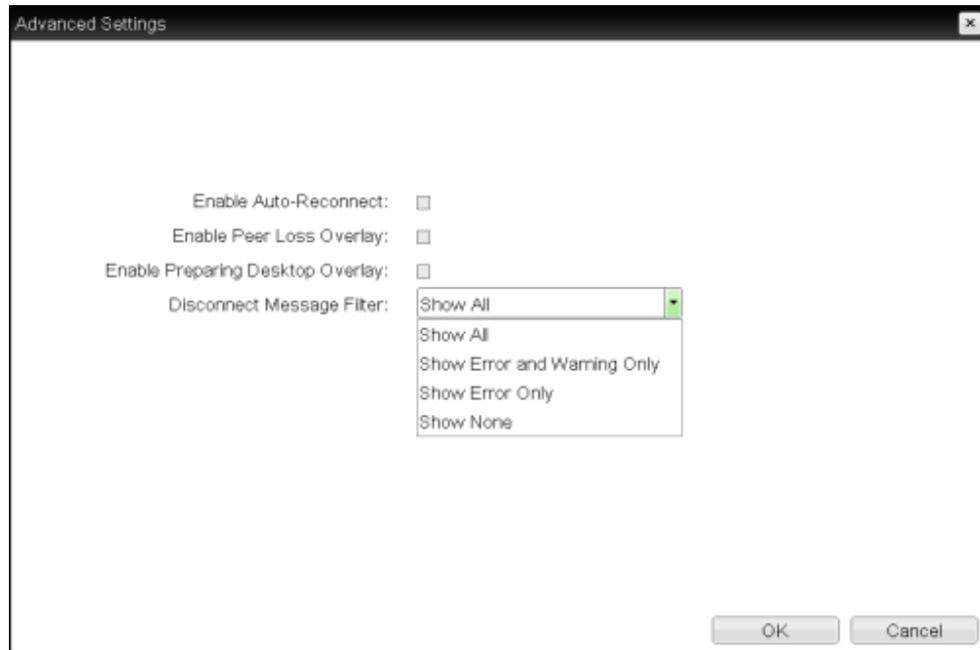


図 5-33 : Advanced Settings

表 5-36 : OSD Session ページパラメータ

パラメータ	説明
Enable Auto-Reconnect	有効になっている場合は、セッションが失われたときに、クライアントが自動的に最後に接続していたホストに再接続します。
Enable Peer Loss Overlay	有効になっている場合は、ネットワーク接続の消失が検出されたときに、“Network Connection Lost”オーバーレイがディスプレイ上に表示されます。このオーバーレイは VMware View などの仮想デスクトップの場合にも表示されます。通常のハイパーバイザスケジューリングの遅延によってもこのメッセージが誤ってトリガーされる場合があります。 注意：このオプションはゼロクライアントに対してしか使用することができません。ピア消失通知が必要なデスクトップアプリケーションは、OSD、AWI、または MC を介してこの機能を再有効化する必要があります。
Enable Preparing Desktop Overlay	有効になっている場合は、ユーザがログインしたときに、“Preparing Desktop”オーバーレイがディスプレイ上に表示されます。 注意：このオーバーレイは、デスクトップの表示に数秒以上かかっている場合でもログインが進行中であることを保証します。
Disconnect Message Filter	このフィールドを使用すれば、セッションが切断されたときに表示されるメッセージのタイプを制御することができます。次の 3 つのカテゴリに分かれています。

パラメータ	説明
	<p>情報：セッションに影響を与えるユーザまたは管理者によるアクション：</p> <ul style="list-style-type: none"> • 別の場所からログインしたか、ホストがシャットダウンまたは再起動されたために切断されました。 • 管理者が切断を実行したために切断されました。 • 別の場所からログインしたために切断されました。 • ワークステーションを切断したために切断されました。 <p>警告：セッションに影響を与えるシステムによる予想されるアクション：</p> <ul style="list-style-type: none"> • セッションがタイムアウトしたために切断されました。 <p>エラー：セッションの失敗を引き起こす予期せぬシステムによるアクション：</p> <ul style="list-style-type: none"> • 切断されました。 • 接続できません (0x1001)。IT 管理者に連絡してください。 • 接続できません (0x1002)。IT 管理者に連絡してください。 • セッションがリモートで閉じられました。 • セッションがリモートで閉じられました (原因不明)。 • 設定エラーが原因で切断されました (0x100)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x201)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x300)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x301)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x302)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x303)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x305)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x400)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x401)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x402)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x403)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x404)。IT 管理者に支援を要請してください。 <p>以下の表示を選択することができます。</p> <ol style="list-style-type: none"> 1. Show All messages – このオプションは、情報メッセージ、警告メッセージ、およびエラーメッセージを含むすべての切断メッセ

パラメータ	説明
	<p>ージを表示します。</p> <p>2. Show Error and Warnings Only – このオプションは情報メッセージを表示せず、エラーメッセージと警告メッセージのみを表示します。</p> <p>3. Show Error Only – このオプションは情報メッセージと警告メッセージを表示せず、エラーメッセージのみを表示します。</p> <p>4. Show None – どの切断メッセージも表示しません。</p>

5.6.20 OSD : View Connection Server セッション設定

VMware View Connection Server を使用して仮想デスクトップに接続するようにクライアントを設定する場合は、**Options > Configuration > Session** ページで **View Connection Server** セッション接続タイプを選択します。

このオプションの詳細設定を構成するには、**Advanced** ボタンをクリックします。

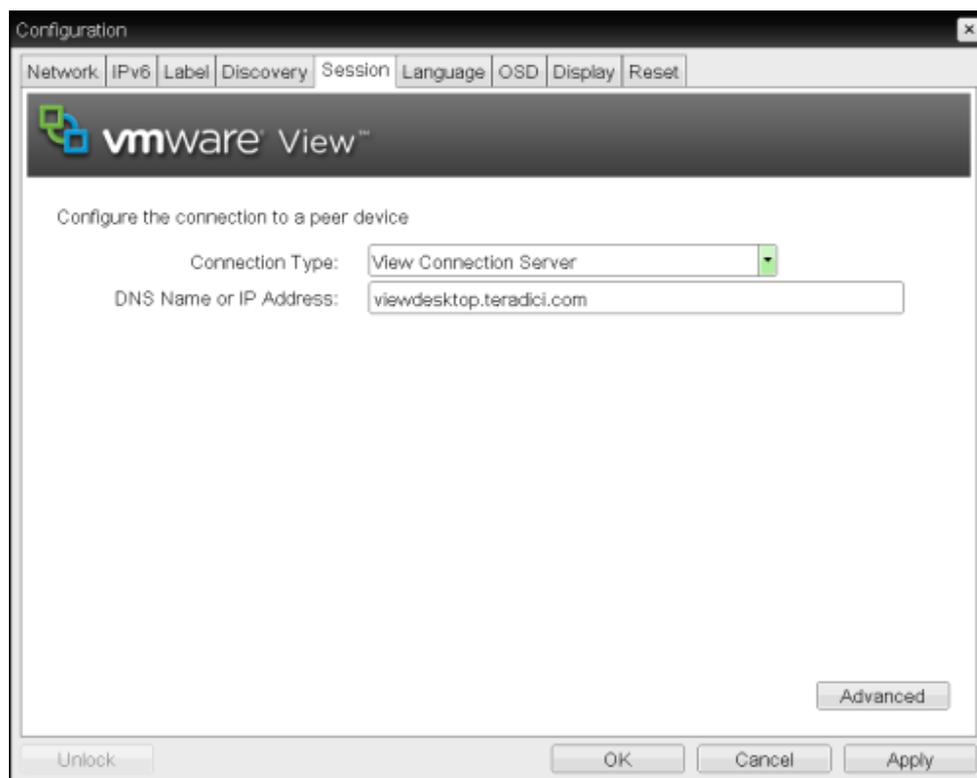


図 5-34 : OSD セッション接続タイプ – View Connection Server

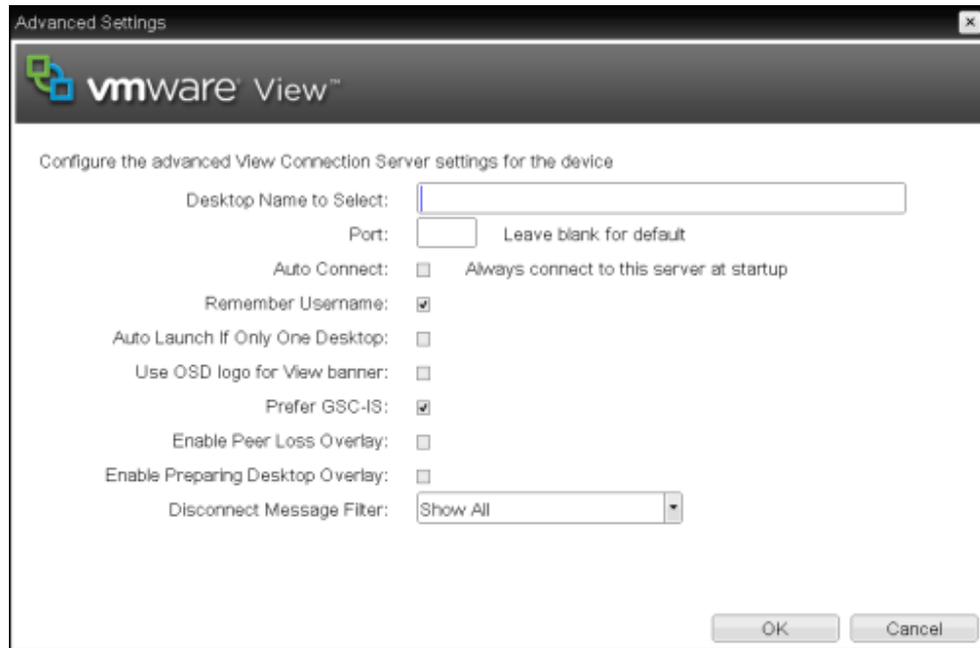


図 5-35 : Advanced Settings

表 5-37 : OSD Session ページパラメータ

パラメータ	説明
DNS Name or IP Address	VMware View Connection Server の DNS 名または IP アドレスを入力します。
Desktop Name to Select	セッションを開始するときにクライアントが使用するプール/デスクトップ名を入力します。 注意：この設定は省略可能です。
Port	デフォルトで、このフィールドは空白になっており、View Connection Server との通信にはポート 443 が使用されます。ネットワークがセキュア接続用として非標準ポートを使用するようにセットアップされている場合は、ポート番号を入力します。
Auto Connect	有効になっている場合は、クライアントが、電源がオンになっているときはいつでも、または、仮想デスクトップとのセッションが終了したときに、自動的に、選択された View Connection Server に接続します。 注意：Auto Connect を有効にしたら、変更を反映させるためにクライアントの電源を入れ直す必要があります。
Remember Username	有効になっている場合は、ユーザ名テキストボックスに、自動的に、最後に入力されたユーザ名が設定されます。

パラメータ	説明
Use OSD Logo for View Banner	有効になっている場合は、ログイン中に、VMware View バナーの代わりに、PCoIP ゼロクライアント OSD ロゴが表示されます。OSD ロゴは OSD Logo Upload ページでアップロードすることができます。
Prefer GSC-IS	選択されている場合は、スマートカードで CAC (GSC-IS) や PIV エンドポイントなどの複数のインターフェースがサポートされていれば、GSC-IS インターフェースが使用されます。スマートカードで CAC と PIV エンドポイントのどちらかなどの 1 つのインターフェースしかサポートされていない場合は、この設定に関係なく、CAC または PIV エンドポイントインターフェースのみが使用されます。これは、PCoIP セッション以外で実行されるスマートカードアクセスにのみ影響を与えます。
Enable Peer Loss Overlay	<p>有効になっている場合は、ネットワーク接続の消失が検出されたときに、“Network Connection Lost”オーバーレイがディスプレイ上に表示されます。このオーバーレイは VMware View などの仮想デスクトップの場合にも表示されます。通常のハイパーバイザスケジューリングの遅延によってもこのメッセージが誤ってトリガーされる場合があります。</p> <p>注意：このオプションはゼロクライアントに対してしか使用することができません。ピア消失通知が必要なデスクトップアプリケーションは、OSD、AWI、または MC を介してこの機能を再有効化する必要があります。</p>
Enable Preparing Desktop Overlay	<p>有効になっている場合は、ユーザがログインしたときに、“Preparing Desktop”オーバーレイがディスプレイ上に表示されます。</p> <p>注意：このオーバーレイは、デスクトップの表示に数秒以上かかっている場合でもログインが進行中であることを保証します。</p>
Disconnect Message Filter	<p>このフィールドを使用すれば、セッションが切断されたときに表示されるメッセージのタイプを制御することができます。次の 3 つのカテゴリに分かれています。</p> <p>情報：セッションに影響を与えるユーザまたは管理者によるアクション：</p> <ul style="list-style-type: none"> • 別の場所からログインしたか、ホストがシャットダウンまたは再起動されたために切断されました。 • 管理者が切断を実行したために切断されました。 • 別の場所からログインしたために切断されました。 • ワークステーションを切断したために切断されました。 <p>警告：セッションに影響を与えるシステムによる予想されるアクション：</p> <ul style="list-style-type: none"> • セッションがタイムアウトしたために切断されました。 <p>エラー：セッションの失敗を引き起こす予期せぬシステムによるアクション：</p> <ul style="list-style-type: none"> • 切断されました。

パラメータ	説明
	<ul style="list-style-type: none"> • 接続できません (0x1001)。IT 管理者に連絡してください。 • 接続できません (0x1002)。IT 管理者に連絡してください。 • セッションがリモートで閉じられました。 • セッションがリモートで閉じられました (原因不明)。 • 設定エラーが原因で切断されました (0x100)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x201)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x300)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x301)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x302)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x303)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x305)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x400)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x401)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x402)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x403)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x404)。IT 管理者に支援を要請してください。 <p>以下の表示を選択することができます。</p> <ol style="list-style-type: none"> 1. Show All messages – このオプションは、情報メッセージ、警告メッセージ、およびエラーメッセージを含むすべての切断メッセージを表示します。 2. Show Error and Warnings Only – このオプションは情報メッセージを表示せず、エラーメッセージと警告メッセージのみを表示します。 3. Show Error Only – このオプションは情報メッセージと警告メッセージを表示せず、エラーメッセージのみを表示します。 4. Show None – どの切断メッセージも表示しません。

5.6.21 OSD : View Connection Server + 自動ログオンセッション設定

ユーザが VMware View Connection Server 経由で仮想デスクトップに接続するときに自動的にユーザのログイン詳細を入力するようにクライアントを設定する場合は、

Options > Configuration > Session ページで **View Connection Server + 自動ログオン** セッション接続タイプを選択します。

このオプションの詳細設定を構成するには、**Advanced** ボタンをクリックします。

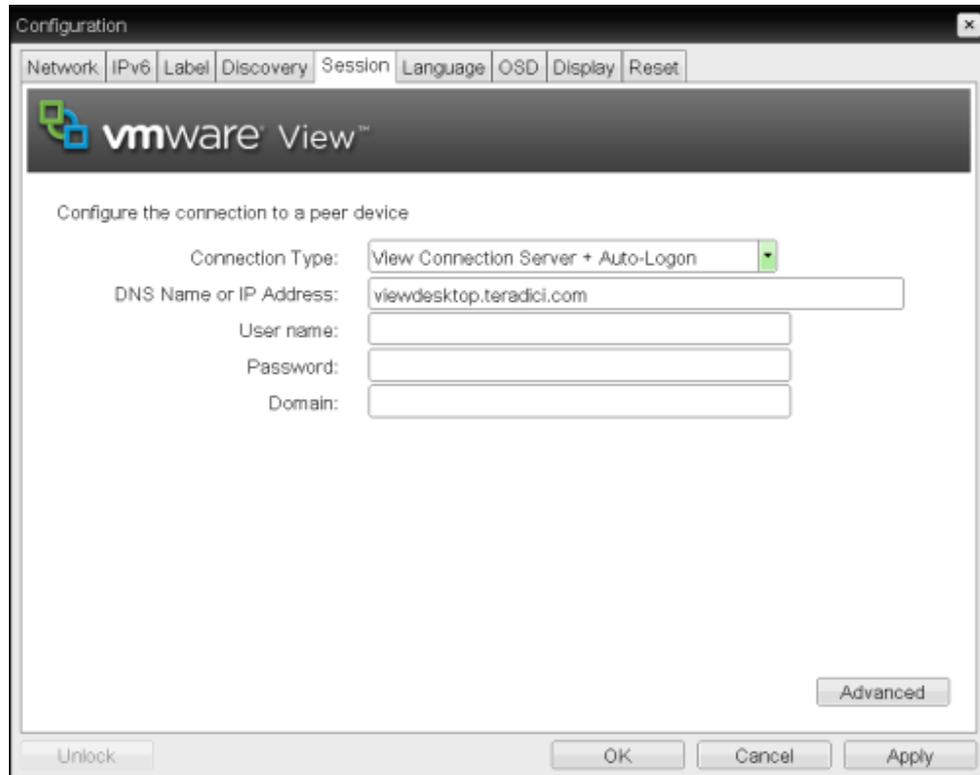


図 5-36 : OSD セッション接続タイプ – View Connection Server + 自動ログオン

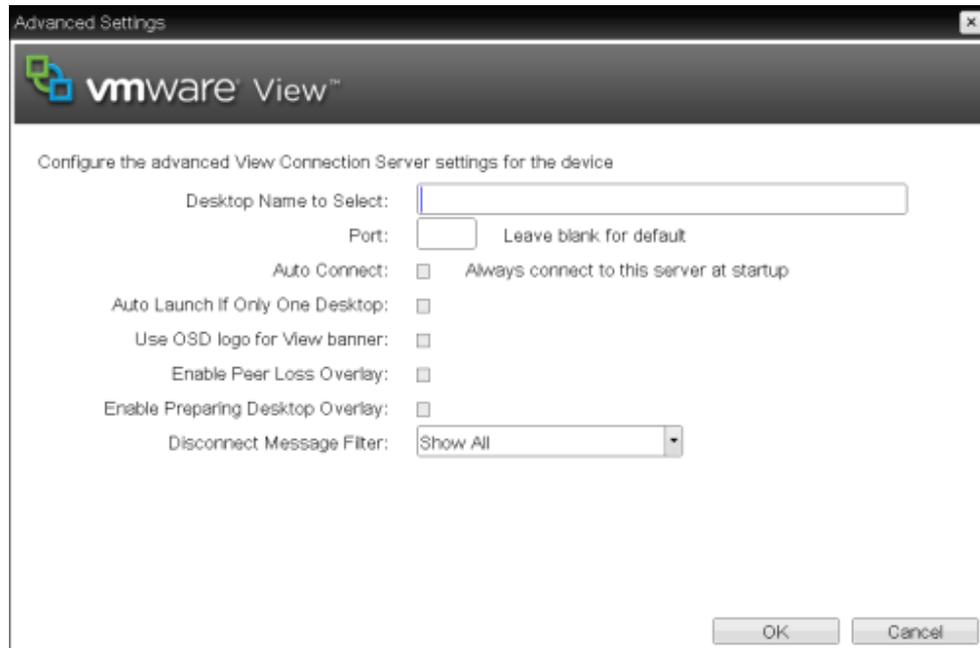


図 5-37 : Advanced Settings

表 5-38 : OSD Session ページパラメータ

パラメータ	説明
DNS Name or IP Address	VMware View Connection Server の DNS 名または IP アドレスを入力します。
User name	クライアントのユーザ名を入力します。
Password	クライアントのパスワードを入力します。
Domain	クライアントのドメイン名を入力します。
Desktop Name to Select	セッションを開始するときにクライアントが使用するプール/デスクトップ名を入力します。 注意：この設定は省略可能です。
Port	デフォルトで、このフィールドは空白になっており、View Connection Server との通信にはポート 443 が使用されます。ネットワークがセキュア接続用として非標準ポートを使用するようにセットアップされている場合は、ポート番号を入力します。
Auto Connect	有効になっている場合は、クライアントが、電源がオンになっているときはいつでも、または、仮想デスクトップとのセッションが終了したときに、自動的に、選択された View Connection Server に接続し

パラメータ	説明
	<p>ます。</p> <p>注意： Auto Connect を有効にしたら、変更を反映させるためにクライアントの電源を入れ直す必要があります。</p>
Auto Launch If Only One Desktop	<p>有効になっている場合は、ユーザ資格情報の入力後に、自動的に、ユーザが仮想デスクトップに接続されます。</p> <p>注意：この機能は、単一のデスクトップを使用可能なユーザにのみ適用されます。複数の仮想デスクトップを使用可能なユーザには適用されません。</p>
Use OSD Logo for View Banner	<p>有効になっている場合は、ログイン中に、VMware View バナーの代わりに、PCoIP ゼロクライアント OSD ロゴが表示されます。OSD ロゴは OSD Logo Upload ページでアップロードすることができます。</p>
Enable Peer Loss Overlay	<p>有効になっている場合は、ネットワーク接続の消失が検出されたときに、“Network Connection Lost”オーバーレイがディスプレイ上に表示されます。このオーバーレイは VMware View などの仮想デスクトップの場合にも表示されます。通常のハイパーバイザスケジューリングの遅延によってもこのメッセージが誤ってトリガーされる場合があります。</p> <p>注意：このオプションはゼロクライアントに対してしか使用することができません。ピア消失通知が必要なデスクトップアプリケーションは、OSD、AWI、または MC を介してこの機能を再有効化する必要があります。</p>
Enable Preparing Desktop Overlay	<p>有効になっている場合は、ユーザがログインしたときに、“Preparing Desktop”オーバーレイがディスプレイ上に表示されます。</p> <p>注意：このオーバーレイは、デスクトップの表示に数秒以上かかっている場合でもログインが進行中であることを保証します。</p>
Disconnect Message Filter	<p>このフィールドを使用すれば、セッションが切断されたときに表示されるメッセージのタイプを制御することができます。次の 3 つのカテゴリに分かれています。</p> <p>情報：セッションに影響を与えるユーザまたは管理者によるアクション：</p> <ul style="list-style-type: none"> • 別の場所からログインしたか、ホストがシャットダウンまたは再起動されたために切断されました。 • 管理者が切断を実行したために切断されました。 • 別の場所からログインしたために切断されました。 • ワークステーションを切断したために切断されました。 <p>警告：セッションに影響を与えるシステムによる予想されるアクション：</p> <ul style="list-style-type: none"> • セッションがタイムアウトしたために切断されました。 <p>エラー：セッションの失敗を引き起こす予期せぬシステムによるアク</p>

パラメータ	説明
	<p>セッション：</p> <ul style="list-style-type: none"> • 切断されました。 • 接続できません (0x1001)。IT 管理者に連絡してください。 • 接続できません (0x1002)。IT 管理者に連絡してください。 • セッションがリモートで閉じられました。 • セッションがリモートで閉じられました (原因不明)。 • 設定エラーが原因で切断されました (0x100)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x201)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x300)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x301)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x302)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x303)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x305)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x400)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x401)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x402)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x403)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x404)。IT 管理者に支援を要請してください。 <p>以下の表示を選択することができます。</p> <ol style="list-style-type: none"> 1. Show All messages – このオプションは、情報メッセージ、警告メッセージ、およびエラーメッセージを含むすべての切断メッセージを表示します。 2. Show Error and Warnings Only – このオプションは情報メッセージを表示せず、エラーメッセージと警告メッセージのみを表示します。 3. Show Error Only – このオプションは情報メッセージと警告メッセージを表示せず、エラーメッセージのみを表示します。 4. Show None – どの切断メッセージも表示しません。

5.6.22 OSD : View Connection Server + キオスクセッション設定

VMware View Connection Server を介して仮想デスクトップに接続するときにキオスクモードを使用するようにクライアントを設定する場合は、**Options > Configuration > Session** ページで **View Connection Server + キオスクセッション** 接続タイプを選択します。

このオプションの詳細設定を構成するには、**Advanced** ボタンをクリックします。

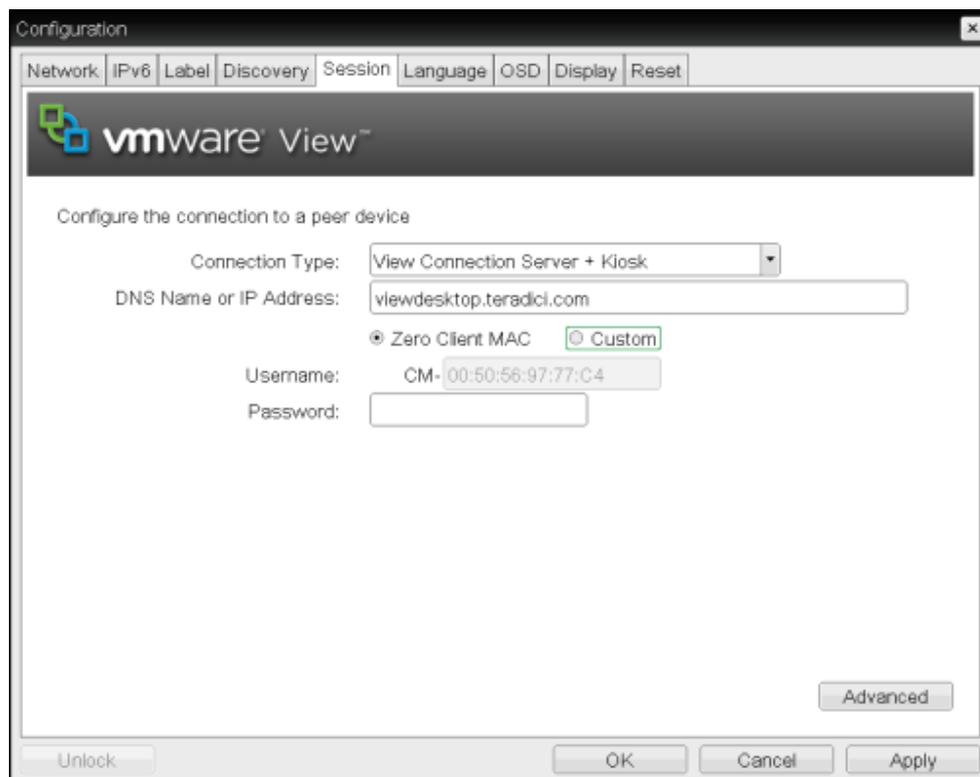


図 5-38 : OSD セッション接続タイプ – View Connection Server + キオスク

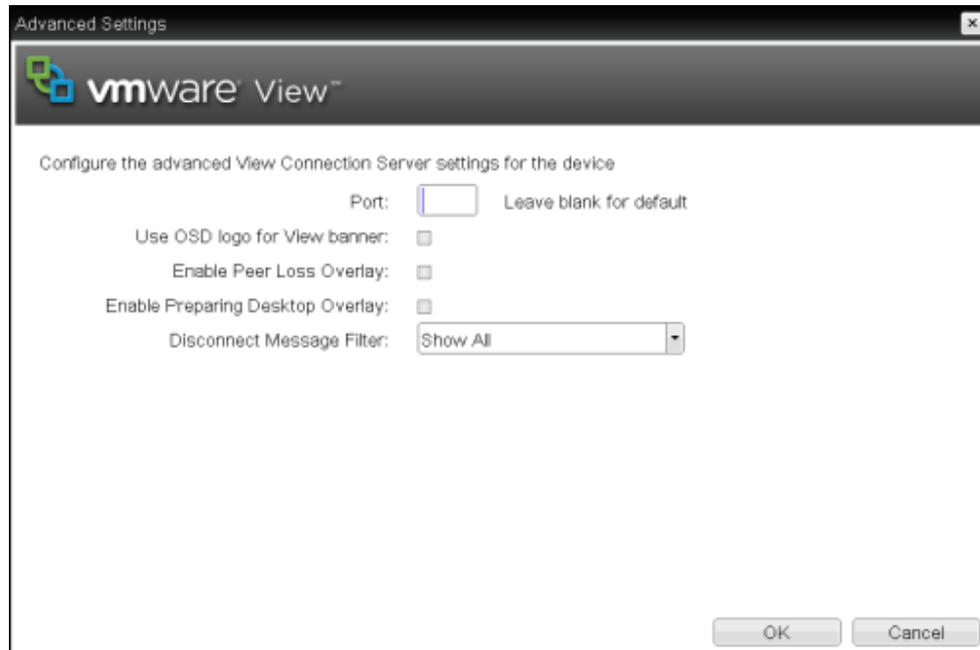


図 5-39 : Advanced Settings

表 5-39 : OSD Session ページパラメータ

パラメータ	説明
DNS Name or IP Address	VMware View Connection Server の DNS 名または IP アドレスを入力します。
Username Type	View Connection Server 上でデバイスに使用するネーミングにマッチしたユーザ名のタイプを選択します。 <ul style="list-style-type: none"> • Zero Client MAC : このオプションは、自動的に、Username フィールドにゼロクライアントの MAC アドレスを設定する場合に選択します。 • Custom : ゼロクライアントのユーザ名を入力します。このユーザ名にはプレフィックスの"Custom"が付加されます。
Username	ユーザ名タイプとして Custom が選択されている場合に、このカスタムユーザ名要素の値を入力します。このフィールドは最大 13 文字に制限されています。
Password	キオスクに対して仮想マシンをパスワードで保護する場合に、このフィールドにパスワードを入力します。このパスワードは、 View Connection Server でデバイスに対して入力されたものと同じにする必要があります。
Port	デフォルトで、このフィールドは空白になっており、 View Connection Server との通信にはポート 443 が使用されます。

パラメータ	説明
	ネットワークがセキュア接続用として非標準ポートを使用するようにセットアップされている場合は、ポート番号を入力します。
Use OSD Logo for View Banner	有効になっている場合は、ログイン中に、VMware View バナーの代わりに、PCoIP ゼロクライアント OSD ロゴが表示されます。OSD ロゴは OSD Logo Upload ページでアップロードすることができます。
Enable Peer Loss Overlay	<p>有効になっている場合は、ネットワーク接続の消失が検出されたときに、“Network Connection Lost”オーバーレイがディスプレイ上に表示されます。このオーバーレイは VMware View などの仮想デスクトップの場合にも表示されます。通常のハイパーバイザスケジューリングの遅延によってもこのメッセージが誤ってトリガーされる場合があります。</p> <p>注意：このオプションはゼロクライアントに対してしか使用することができません。ピア消失通知が必要なデスクトップアプリケーションは、OSD、AWI、または MC を介してこの機能を再有効化する必要があります。</p>
Enable Preparing Desktop Overlay	<p>有効になっている場合は、ユーザがログインしたときに、“Preparing Desktop”オーバーレイがディスプレイ上に表示されます。</p> <p>注意：このオーバーレイは、デスクトップの表示に数秒以上かかっている場合でもログインが進行中であることを保証します。</p>
Disconnect Message Filter	<p>このフィールドを使用すれば、セッションが切断されたときに表示されるメッセージのタイプを制御することができます。次の 3 つのカテゴリに分かれています。</p> <p>情報：セッションに影響を与えるユーザまたは管理者によるアクション：</p> <ul style="list-style-type: none"> • 別の場所からログインしたか、ホストがシャットダウンまたは再起動されたために切断されました。 • 管理者が切断を実行したために切断されました。 • 別の場所からログインしたために切断されました。 • ワークステーションを切断したために切断されました。 <p>警告：セッションに影響を与えるシステムによる予想されるアクション：</p> <ul style="list-style-type: none"> • セッションがタイムアウトしたために切断されました。 <p>エラー：セッションの失敗を引き起こす予期せぬシステムによるアクション：</p> <ul style="list-style-type: none"> • 切断されました。 • 接続できません (0x1001)。IT 管理者に連絡してください。 • 接続できません (0x1002)。IT 管理者に連絡してください。 • セッションがリモートで閉じられました。 • セッションがリモートで閉じられました (原因不明)。 • 設定エラーが原因で切断されました (0x100)。IT 管理者に支援

パラメータ	説明
	<p>を要請してください。</p> <ul style="list-style-type: none"> • 設定エラーが原因で切断されました (0x201)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x300)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x301)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x302)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x303)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x305)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x400)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x401)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x402)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x403)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x404)。IT 管理者に支援を要請してください。 <p>以下の表示を選択することができます。</p> <ol style="list-style-type: none"> 1. Show All messages – このオプションは、情報メッセージ、警告メッセージ、およびエラーメッセージを含むすべての切断メッセージを表示します。 2. Show Error and Warnings Only – このオプションは情報メッセージを表示せず、エラーメッセージと警告メッセージのみを表示します。 3. Show Error Only – このオプションは情報メッセージと警告メッセージを表示せず、エラーメッセージのみを表示します。 4. Show None – どの切断メッセージも表示しません。

5.6.23 OSD : View Connection Server + Imprivata OneSign セッション設定

仮想デスクトップに接続するときに View Connection Server に加えて Imprivata OneSign システム経由でも認証するようにクライアントを設定する場合は、**Options > Configuration > Session** ページで **View Connection Server + Imprivata OneSign** セッション接続タイプを選択します。

このオプションの詳細設定を構成するには、**Advanced** ボタンをクリックします。

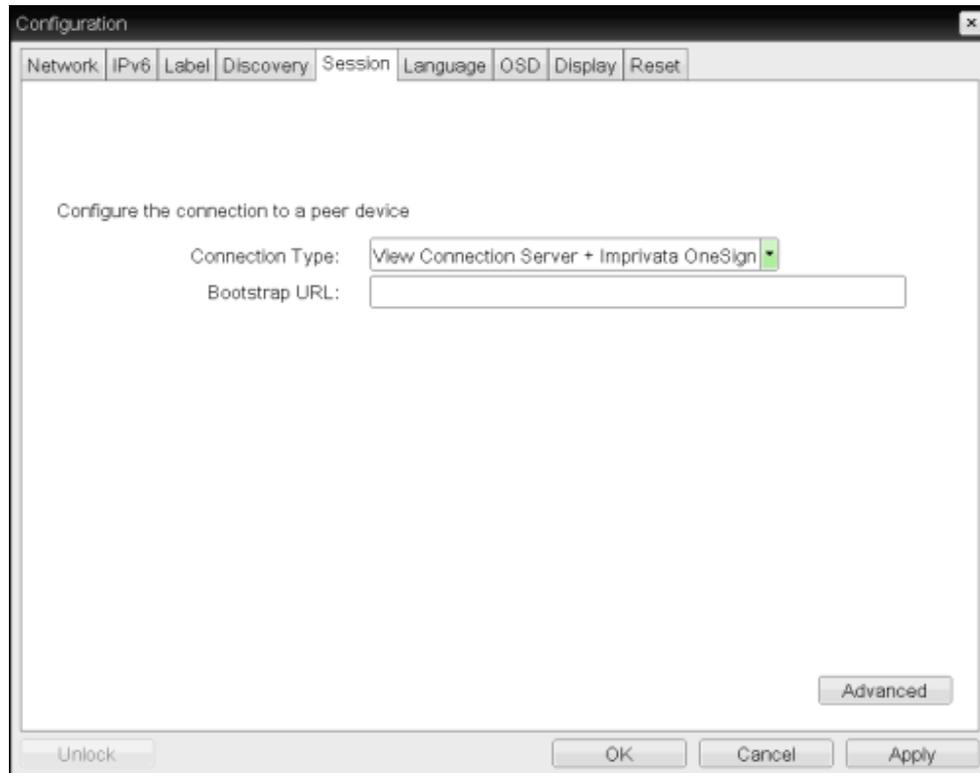


図 5-40 : OSD セッション接続タイプ – View Connection Server + Imprivata OneSign

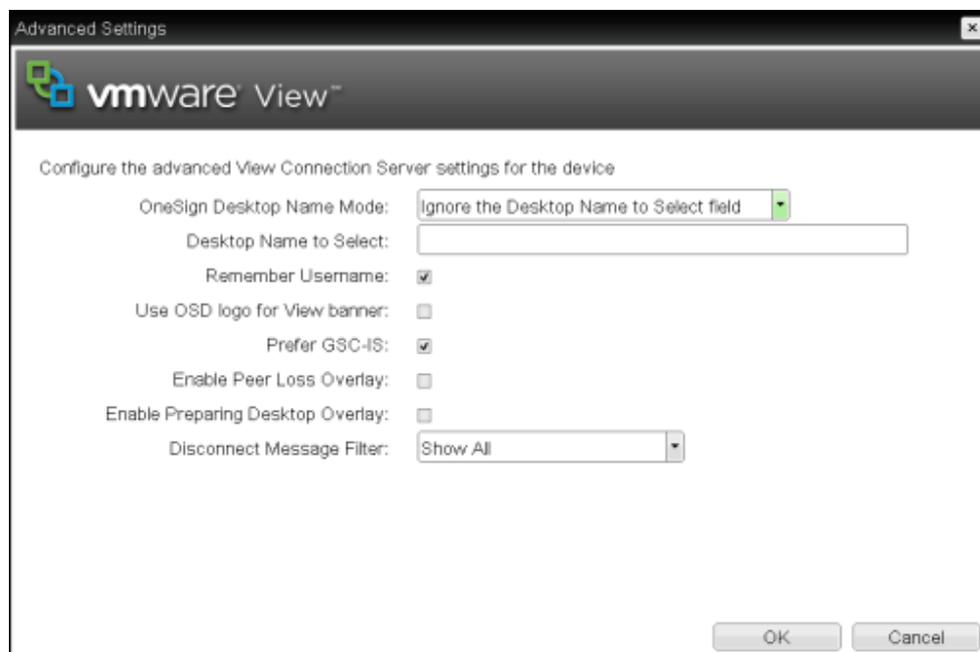


図 5-41 : Advanced Settings

表 5-40 : OSD Session ページパラメータ

パラメータ	説明
DNS Name or IP Address	VMware View Connection Server の DNS 名または IP アドレスを入力します。
Bootstrap URL	OneSign 認証デプロイメント内で初期 OneSign サーバを探すために使用されるブートストラップ URL を入力します。
Onesign Desktop Name Mode	Desktop Name to Select プロパティが OneSign モードで使用されるかどうかを選択します。 <ul style="list-style-type: none"> • Ignore the Desktop Name to Select field • Use the Desktop Name to Select field if set
Desktop Name to Select	デスクトップ名を入力します。デスクトッププールリストにこの名前のプールが含まれている場合は、クライアントが即座にそのプールを使用したセッションを開始します。 注意：このフィールドは大文字と小文字が区別されます。
Remember Username	有効になっている場合は、ユーザ名テキストボックスに、自動的に、最後に入力されたユーザ名が設定されます。
Use OSD Logo for View Banner	有効になっている場合は、ログイン中に、VMware View バナーの代わりに、PCoIP ゼロクライアント OSD ロゴが表示されます。OSD ロゴは OSD Logo Upload ページでアップロードすることができます。
Prefer GSC-IS	選択されている場合は、スマートカードで CAC (GSC-IS) や PIV エンドポイントなどの複数のインターフェースがサポートされていれば、GSC-IS インターフェースが使用されます。スマートカードで CAC と PIV エンドポイントのどちらかなどの 1 つのインターフェースしかサポートされていない場合は、この設定に関係なく、CAC または PIV エンドポイントインターフェースのみが使用されます。これは、PCoIP セッション以外で実行されるスマートカードアクセスにのみ影響を与えます。
Enable Peer Loss Overlay	有効になっている場合は、ネットワーク接続の消失が検出されたときに、“Network Connection Lost”オーバーレイがディスプレイ上に表示されます。このオーバーレイは VMware View などの仮想デスクトップの場合にも表示されます。通常のハイパーバイザスケジューリングの遅延によってもこのメッセージが誤ってトリガーされる場合があります。 注意：このオプションはゼロクライアントに対してしか使用することができません。ピア消失通知が必要なデスクトップアプリケーションは、OSD、AWI、または MC を介してこの機能を再有効化する必要があります。

パラメータ	説明
<p>Enable Preparing Desktop Overlay</p>	<p>有効になっている場合は、ユーザがログインしたときに、"Preparing Desktop"オーバーレイがディスプレイ上に表示されます。</p> <p>注意：このオーバーレイは、デスクトップの表示に数秒以上かかっている場合でもログインが進行中であることを保証します。</p>
<p>Disconnect Message Filter</p>	<p>このフィールドを使用すれば、セッションが切断されたときに表示されるメッセージのタイプを制御することができます。次の3つのカテゴリに分かれています。</p> <p>情報：セッションに影響を与えるユーザまたは管理者によるアクション：</p> <ul style="list-style-type: none"> • 別の場所からログインしたか、ホストがシャットダウンまたは再起動されたために切断されました。 • 管理者が切断を実行したために切断されました。 • 別の場所からログインしたために切断されました。 • ワークステーションを切断したために切断されました。 <p>警告：セッションに影響を与えるシステムによる予想されるアクション：</p> <ul style="list-style-type: none"> • セッションがタイムアウトしたために切断されました。 <p>エラー：セッションの失敗を引き起こす予期せぬシステムによるアクション：</p> <ul style="list-style-type: none"> • 切断されました。 • 接続できません (0x1001)。IT 管理者に連絡してください。 • 接続できません (0x1002)。IT 管理者に連絡してください。 • セッションがリモートで閉じられました。 • セッションがリモートで閉じられました (原因不明)。 • 設定エラーが原因で切断されました (0x100)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x201)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x300)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x301)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x302)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x303)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x305)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x400)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x401)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x402)。IT 管理者に支援を要請してください。

パラメータ	説明
	<p>を要請してください。</p> <ul style="list-style-type: none"> • 設定エラーが原因で切断されました (0x403)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x404)。IT 管理者に支援を要請してください。 <p>以下の表示を選択することができます。</p> <ol style="list-style-type: none"> 1. Show All messages – このオプションは、情報メッセージ、警告メッセージ、およびエラーメッセージを含むすべての切断メッセージを表示します。 2. Show Error and Warnings Only – このオプションは情報メッセージを表示せず、エラーメッセージと警告メッセージのみを表示します。 3. Show Error Only – このオプションは情報メッセージと警告メッセージを表示せず、エラーメッセージのみを表示します。 4. Show None – どの切断メッセージも表示しません。

5.6.24 OSD : Connection Management Interface セッション設定

外部接続マネージャをクライアントが使用する [コネクションブローカ](#) として設定する場合は、**Options > Configuration > Session** ページで **Connection Management Interface** セッション接続タイプを選択します。

注意：外部接続マネージャは大規模で複雑なシステムの管理手順を簡略化することができます。管理接続では、外部接続マネージャサーバがデバイスと通信して、それをリモートで制御および設定することができます。コネクションマネージャは、接続するデバイスに適切なピアを特定してから接続を開始することもできます。

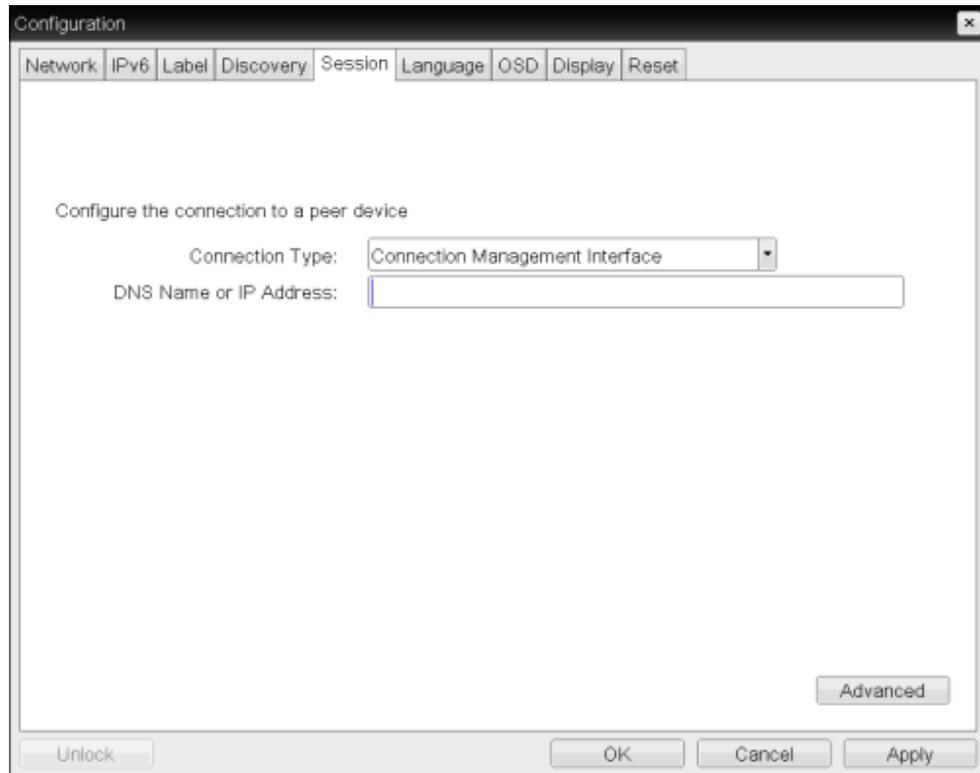


図 5-42 : OSD セッション接続タイプ - Connection Management Interface

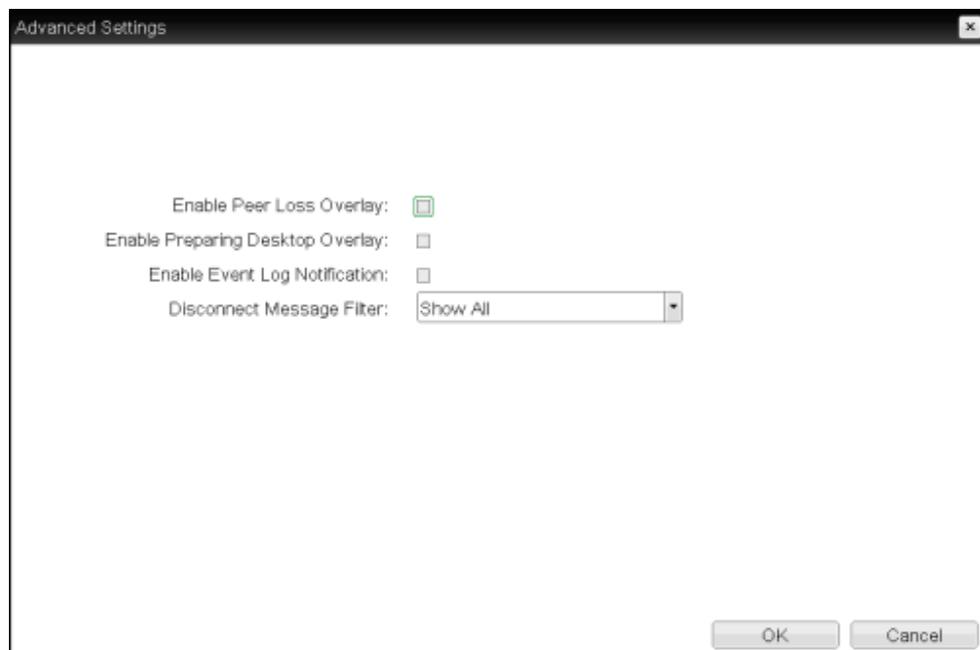


図 5-43 : Advanced Settings

表 5-41 : AWI Session ページパラメータ

パラメータ	説明
DNS Name or IP Address	コネクションマネージャの DNS 名または IP アドレスを入力します。
Enable Peer Loss Overlay	<p>有効になっている場合は、ネットワーク接続の消失が検出されたときに、“Network Connection Lost”オーバーレイがディスプレイ上に表示されます。このオーバーレイは VMware View などの仮想デスクトップの場合にも表示されます。通常のハイパーバイザスケジューリングの遅延によってもこのメッセージが誤ってトリガーされる場合があります。</p> <p>注意：このオプションはゼロクライアントに対してしか使用することができません。ピア消失通知が必要なデスクトップアプリケーションは、OSD、AWI、または MC を介してこの機能を再有効化する必要があります。</p>
Enable Preparing Desktop Overlay	<p>有効になっている場合は、ユーザがログインしたときに、“Preparing Desktop”オーバーレイがディスプレイ上に表示されます。</p> <p>注意：このオーバーレイは、デスクトップの表示に数秒以上かかっている場合でもログインが進行中であることを保証します。</p>
Enable Event Log Notification	有効になっている場合は、クライアントがそのイベントログの内容を接続管理サーバに送信します。
Disconnect Message Filter	<p>このフィールドを使用すれば、セッションが切断されたときに表示されるメッセージのタイプを制御することができます。次の 3 つのカテゴリに分かれています。</p> <p>情報：セッションに影響を与えるユーザまたは管理者によるアクション：</p> <ul style="list-style-type: none"> 別の場所からログインしたか、ホストがシャットダウンまたは再起動されたために切断されました。 管理者が切断を実行したために切断されました。 別の場所からログインしたために切断されました。 ワークステーションを切断したために切断されました。 <p>警告：セッションに影響を与えるシステムによる予想されるアクション：</p> <ul style="list-style-type: none"> セッションがタイムアウトしたために切断されました。 <p>エラー：セッションの失敗を引き起こす予期せぬシステムによるアクション：</p> <ul style="list-style-type: none"> 切断されました。 接続できません (0x1001)。IT 管理者に連絡してください。 接続できません (0x1002)。IT 管理者に連絡してください。 セッションがリモートで閉じられました。 セッションがリモートで閉じられました (原因不明)。 設定エラーが原因で切断されました (0x100)。IT 管理者に支援

パラメータ	説明
	<p>を要請してください。</p> <ul style="list-style-type: none"> • 設定エラーが原因で切断されました (0x201)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x300)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x301)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x302)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x303)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x305)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x400)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x401)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x402)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x403)。IT 管理者に支援を要請してください。 • 設定エラーが原因で切断されました (0x404)。IT 管理者に支援を要請してください。 <p>以下の表示を選択することができます。</p> <ol style="list-style-type: none"> 1. Show All messages – このオプションは、情報メッセージ、警告メッセージ、およびエラーメッセージを含むすべての切断メッセージを表示します。 2. Show Error and Warnings Only – このオプションは情報メッセージを表示せず、エラーメッセージと警告メッセージのみを表示します。 3. Show Error Only – このオプションは情報メッセージと警告メッセージを表示せず、エラーメッセージのみを表示します。 4. Show None – どの切断メッセージも表示しません。

5.7 セッション暗号化の設定

5.7.1 MC : 暗号化設定

このページの設定を使用すれば、クライアントとホスト間の PCoIP セッションをネゴシエートするために使用される Transport Layer Security (TLS) レベルだけでなく、デバイスで使用される暗号化スキームも使用してプロファイルを構成することができます。少なくとも 1 つの暗号化スキームを有効にする必要があります。

MC でプロパティを有効にするには、**Set in Profile** チェックボックスをオンにし、指示に従ってフィールドを設定します。このページでプロパティを更新したら、**Save** をクリックして変更を保存します。

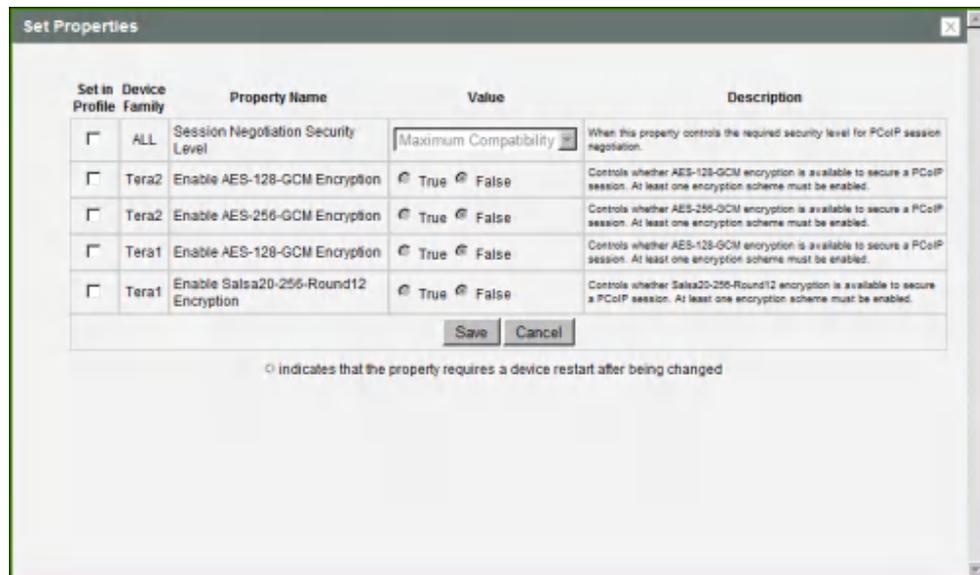


図 5-44 : MC 暗号化設定

表 5-42 : MC 暗号化設定パラメータ

パラメータ	説明
Session Negotiation Security Level	PCoIP セッションネゴシエーションに必要なセキュリティレベルを設定します。 <ul style="list-style-type: none"> • Maximum Compatibility • Suite B : このオプションはより高度なセキュリティを提供します。
Enable AES-128-GCM Encryption (Tera2)	有効になっている場合は、PCoIP セッションの保護に AES-128-GCM 暗号化スキームが使用されます。
Enable AES-256-GCM Encryption (Tera2)	有効になっている場合は、PCoIP セッションの保護に AES-256-GCM 暗号化スキームが使用されます。 注意：この方式では、 Tera2 デバイスのハードウェアエンドポイント間で最高性能を実現することができます。
Enable AES-128-GCM Encryption (Tera1)	有効になっている場合は、PCoIP セッションの保護に AES-128-GCM 暗号化スキームが使用されます。 注意：この方式では、 Tera1 デバイスのハードウェアエンドポイント間で最高性能を実現することができます。

パラメータ	説明
Enable Salsa20-256-Round12 Encryption (Tera1)	有効になっている場合は、PCoIPセッションの保護に Salsa20-256-Round12M 暗号化スキームが使用されます。 注意：この方式では、Tera1 クライアントが VMware 4 以降に接続されており、ネットワーク上で 7 Mbps 以上の速度が利用可能であれば、高い性能を実現できる可能性があります。

5.7.2 AWI：暗号化設定に関するヘルプ

ホストおよびクライアント AWI 用の暗号化設定は、各セッション接続タイプの **Configuration > Session** ページに配置されています。詳細については、以下のトピックに含まれるフィールドの説明を参照してください。

- [AWI ホスト：Direct from Client セッション設定](#)
- [AWI クライアント：Direct to Host セッション設定](#)
- [AWI クライアント：Direct to Host + SLP ホストディスクカバリセッション設定](#)
- [AWI クライアント：View Connection Server セッション設定](#)
- [AWI クライアント：View Connection Server + 自動ログオンセッション設定](#)
- [AWI クライアント：View Connection Server + キオスクセッション設定](#)
- [AWI クライアント：View Connection Server + Imprivata OneSign セッション設定](#)

5.8 セッション帯域幅の設定

5.8.1 MC：帯域幅設定

このページの設定を使用すれば、PCoIP セッション中にホストとクライアントで使用される帯域幅パラメータでプロファイルを設定することができます。

MC でプロパティを有効にするには、**Set in Profile** チェックボックスをオンにし、指示に従ってフィールドを設定します。このページでプロパティを更新したら、**Save** をクリックして変更を保存します。

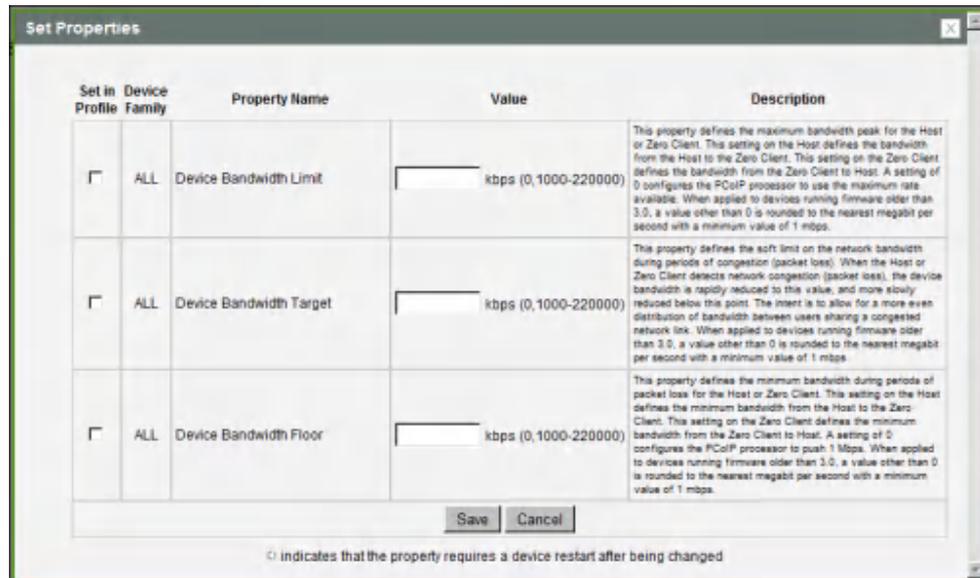


図 5-45 : MC 帯域幅設定

表 5-43 : MC 帯域幅設定パラメータ

パラメータ	説明
Device Bandwidth Limit	<p>ホストまたはクライアントの最大帯域幅ピークを入力します。ホストの構成では、この設定によって、ホストからクライアントへの帯域幅（グラフィックスデータなど）が定義されます。クライアントの構成では、この設定によって、クライアントからホストへの帯域幅（USB データなど）が定義されます。</p> <p>デバイス帯域幅の有効範囲は 1000~220000 Kbps です。</p> <p>PCoIP プロセッサは、Device Bandwidth Limit の最大値までの必要な帯域幅しか使用しないうえ、ネットワークの混雑に応じて帯域幅を動的に調整します。このフィールドを 0 に設定した場合は、そのときにネットワーク上で利用可能な最大速度を使用するように PCoIP プロセッサが設定されます。</p> <p>このフィールドは、クライアントとホストが接続されているネットワークの上限に設定することをお勧めします。</p> <p>注意 : 3.0 より古いファームウェアを実行しているデバイスに適用した場合は、0 以外の値が最も近い Mbps（最小値は 1 Mbps）に丸められます。</p>
Device Bandwidth Target	<p>混雑時のネットワーク帯域幅に対する一時的な制限を入力します。ホストまたはクライアントがパケット損失を検出すると、デバイス帯域幅がこの値まで急激に減少してから、この値を下回るとゆっくり減少します。これにより、混雑したネットワークリンクを共有しているユーザ間の帯域幅がより均等に分散されます。</p> <p>注意 : 3.0 より古いファームウェアを実行しているデバイスに適用した場合は、0 以外の値が最も近い Mbps（最小値は 1 Mbps）に丸められます。</p>

パラメータ	説明
Device Bandwidth Floor	<p>混雑が発生して帯域幅が必要になった場合の最小帯域幅を入力します。これにより、混雑またはパケット損失が判明しているネットワークの性能を最適化することができます。帯域幅が必要ない場合は、使用される帯域幅が下限値未満まで減少します。</p> <p>ホストの構成では、この設定によって、ホストからクライアントへの最小帯域幅（グラフィックデータなど）が定義されます。クライアントの構成では、この設定によって、クライアントからホストへの最小帯域幅（USB データなど）が定義されます。</p> <p>0 に設定した場合は、ネットワーク障害が発生したら 1000 Kbps まで帯域幅を下げるように PCoIP プロセッサが設定されます。これを 0 以外の値に設定する場合は、ネットワークトポロジに精通している必要があります。</p> <p>注意：ファームウェアには、必要な帯域幅に到達するまで、ネットワークの混在が検出されるまで、または Device Bandwidth Limit が満たされるまで、使用帯域幅を増やすスロースタートアルゴリズムが実装されています。このアルゴリズムは、Device Bandwidth Limit と 8000 Kbps の小さい方で開始して、使用帯域幅を数秒以内に増やします。このスロースタートアルゴリズムを使用すれば、低帯域幅シナリオ（WAN シナリオなど）の滑らかなセッション起動が可能になります。PCoIP セッションの起動後は、アルゴリズムによって使用帯域幅が増加したときに、ユーザが一時的に低帯域幅ビデオアーチファクトに気付く可能性があります。</p> <p>注意：3.0 より古いファームウェアを実行しているデバイスに適用した場合は、0 以外の値が最も近い Mbps（最小値は 1 Mbps）に丸められます。</p>

5.8.2 AWI：帯域幅設定

このページの設定を使用すれば、PCoIP セッション中にホストまたはクライアントによって使用される帯域幅を制御することができます。このページは、ホストまたはクライアントの **Configuration > Bandwidth** メニューから表示することができます。このページのパラメータは **Apply** のクリック直後に適用されます。

Bandwidth

Configure the device bandwidth limit, target and floor

Device Bandwidth Limit: kbps (0 = no limit)

Device Bandwidth Target: kbps (0 = disabled)

Device Bandwidth Floor: kbps (0 = use default of 1000 kbps)

図 5-46 : AWI Bandwidth ページ

表 5-44 : AWI 帯域幅パラメータ

パラメータ	説明
Device Bandwidth Limit	<p>ホストまたはクライアントの最大帯域幅ピークを入力します。ホストの構成では、この設定によって、ホストからクライアントへの帯域幅（グラフィックスデータなど）が定義されます。クライアントの構成では、この設定によって、クライアントからホストへの帯域幅（USB データなど）が定義されます。</p> <p>デバイス帯域幅の有効範囲は 1000~220000 Kbps です。</p> <p>PCoIP プロセッサは、Device Bandwidth Limit の最大値までの必要な帯域幅しか使用しないうえ、ネットワークの混雑に応じて帯域幅を動的に調整します。このフィールドを 0 に設定した場合は、そのときにネットワーク上で利用可能な最大速度を使用するように PCoIP プロセッサが設定されます。</p> <p>このフィールドは、クライアントとホストが接続されているネットワークの上限に設定することをお勧めします。</p> <p style="color: green;">注意：3.0 より古いファームウェアを実行しているデバイスに適用した場合は、0 以外の値が最も近い Mbps（最小値は 1 Mbps）に丸められます。</p>
Device Bandwidth Target	<p>混雑時のネットワーク帯域幅に対する一時的な制限を入力します。ホストまたはクライアントがパケット損失を検出すると、デバイス帯域幅がこの値まで急激に減少してから、この値を下回るとゆっくり減少します。これにより、混雑したネットワークリンクを共有しているユーザ間の帯域幅がより均等に分散されます。</p>

パラメータ	説明
	<p>注意：3.0 より古いファームウェアを実行しているデバイスに適用した場合は、0 以外の値が最も近い Mbps（最小値は 1 Mbps）に丸められます。</p>
Device Bandwidth Floor	<p>混雑が発生して帯域幅が必要になった場合の最小帯域幅を入力します。これにより、混雑またはパケット損失が判明しているネットワークの性能を最適化することができます。帯域幅が必要ない場合は、使用される帯域幅が下限値未満まで減少します。</p> <p>ホストの構成では、この設定によって、ホストからクライアントへの最小帯域幅（グラフィックデータなど）が定義されます。クライアントの構成では、この設定によって、クライアントからホストへの最小帯域幅（USB データなど）が定義されます。</p> <p>0 に設定した場合は、ネットワーク障害が発生したら 1000 Kbps まで帯域幅を下げるように PCoIP プロセッサが設定されます。これを 0 以外の値に設定する場合は、ネットワークトポロジに精通している必要があります。</p> <p>注意：ファームウェアには、必要な帯域幅に到達するまで、ネットワークの混在が検出されるまで、または Device Bandwidth Limit が満たされるまで、使用帯域幅を増やすスロースタートアルゴリズムが実装されています。このアルゴリズムは、Device Bandwidth Limit と 8000 Kbps の小さい方で開始して、使用帯域幅を数秒以内に増やします。このスロースタートアルゴリズムを使用すれば、低帯域幅シナリオ（WAN シナリオなど）の滑らかなセッション起動が可能になります。PCoIP セッションの起動後は、アルゴリズムによって使用帯域幅が増加したときに、ユーザが一時的に低帯域幅ビデオアーチファクトに気付く可能性があります。</p> <p>注意：3.0 より古いファームウェアを実行しているデバイスに適用した場合は、0 以外の値が最も近い Mbps（最小値は 1 Mbps）に丸められます。</p>

5.9 言語の設定

5.9.1 MC：言語設定

このページの設定を使用すれば、OSD ユーザインターフェースで使用される言語でプロファイルを設定することができます。

MC でプロパティを有効にするには、**Set in Profile** チェックボックスをオンにし、指示に従ってフィールドを設定します。このページでプロパティを更新したら、**Save** をクリックして変更を保存します。

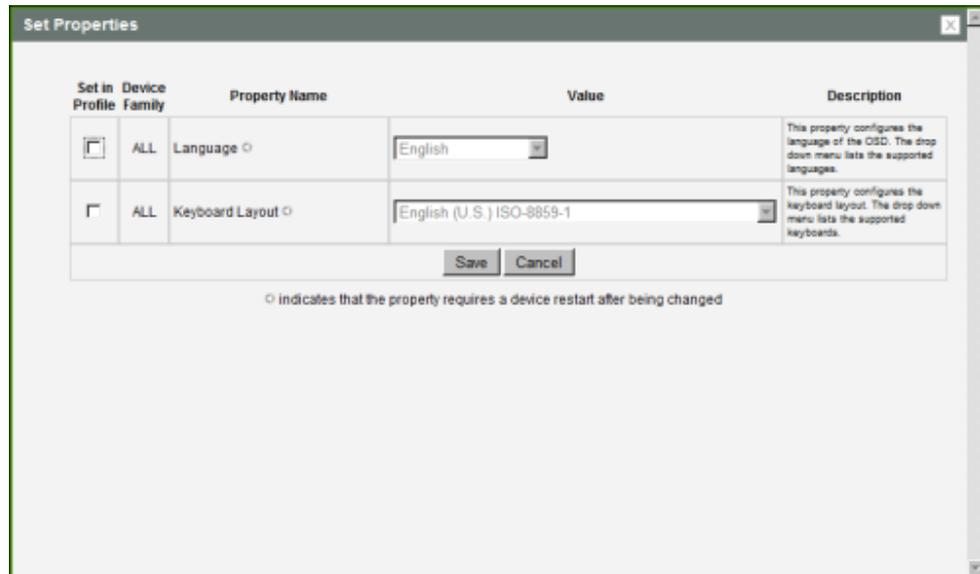


図 5-47 : MC 言語設定

表 5-45 : MC 言語設定パラメータ

パラメータ	説明
Language	OSD ユーザインターフェースに対して設定します。 注意：これは、実際のユーザセッションの言語設定に影響を与えません。 注意：このプロパティを変更した場合はデバイスを再起動する必要があります。
Keyboard Layout	キーボードのレイアウトを変更します。ユーザがセッションを開始すると、この設定が仮想マシンに転送されます。PCoIP "Use Enhanced Keyboard on Windows Client if available" GPO がキーボードレイアウト設定を許可するように設定されている場合は、この設定がユーザのセッション中に使用されます。この GPO がキーボードレイアウト設定を許可するように設定されていない場合は、この設定が無視されます。 注意：このプロパティを変更した場合はデバイスを再起動する必要があります。

5.9.2 AWI クライアント：言語設定

このページの設定を使用すれば、OSD ユーザインターフェースで使用される言語を設定することができます。このページは、**Configuration > Language** メニューから表示することができます。

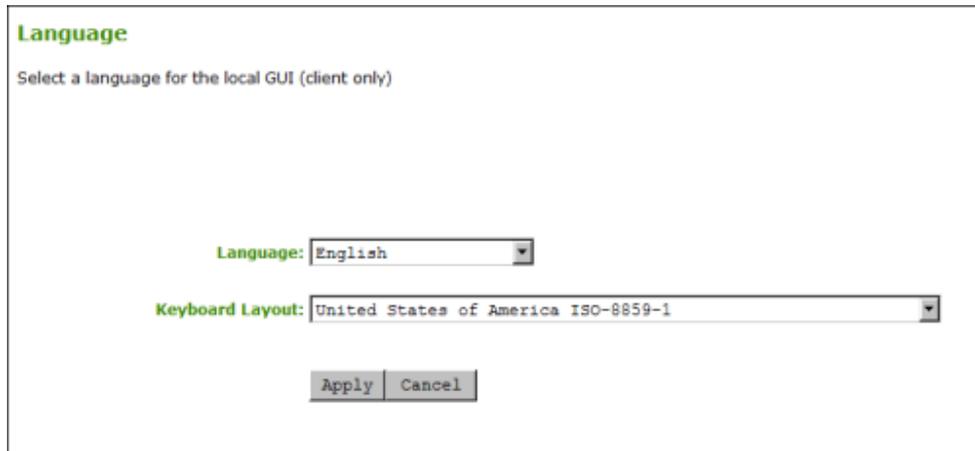


図 5-48 : AWI クライアント Language ページ

表 5-46 : AWI クライアント言語パラメータ

パラメータ	説明
Language	OSD ユーザインターフェースに対して設定します。 注意：これは、実際のユーザセッションの言語設定に影響を与えません。
Keyboard Layout	キーボードのレイアウトを変更します。ユーザがセッションを開始すると、この設定が仮想マシンに転送されます。PCoIP "Use Enhanced Keyboard on Windows Client if available" GPO がキーボードレイアウト設定を許可するように設定されている場合は、この設定がユーザのセッション中に使用されます。この GPO がキーボードレイアウト設定を許可するように設定されていない場合は、この設定が無視されます。

5.9.3 OSD : 言語設定

このページの設定を使用すれば、OSD ユーザインターフェースで使用される言語を設定することができます。このページは、**Options > Configuration > Language** メニューから表示することができます。

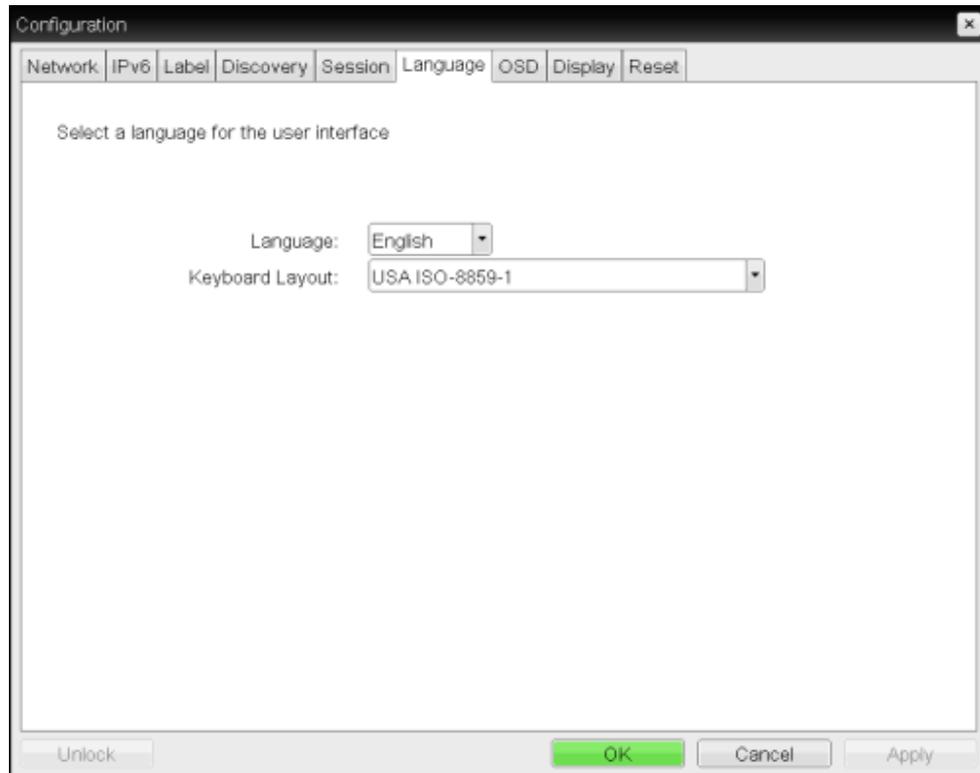


図 5-49 : OSD Language ページ

表 5-47 : OSD 言語パラメータ

パラメータ	説明
Language	OSD ユーザインターフェースに対して設定します。 注意：これは、実際のユーザセッションの言語設定に影響を与えません。
Keyboard Layout	キーボードのレイアウトを変更します。ユーザがセッションを開始すると、この設定が仮想マシンに転送されます。PCoIP "Use Enhanced Keyboard on Windows Client if available" GPO がキーボードレイアウト設定を許可するように設定されている場合は、この設定がユーザのセッション中に使用されます。この GPO がキーボードレイアウト設定を許可するように設定されていない場合は、この設定が無視されます。

5.10 OSD パラメータの設定

5.10.1 MC : OSD 設定

このページの設定を使用すれば、デバイスの OSD 上で使用されるスクリーンセーバタイムアウト値を設定したり、OSD に表示しないメニューとメニュー項目を制御したりするようにプロファイルを構成することができます。

MC でプロパティを有効にするには、**Set in Profile** チェックボックスをオンにし、指示に従ってフィールドを設定します。このページでプロパティを更新したら、**Save** をクリックして変更を保存します。

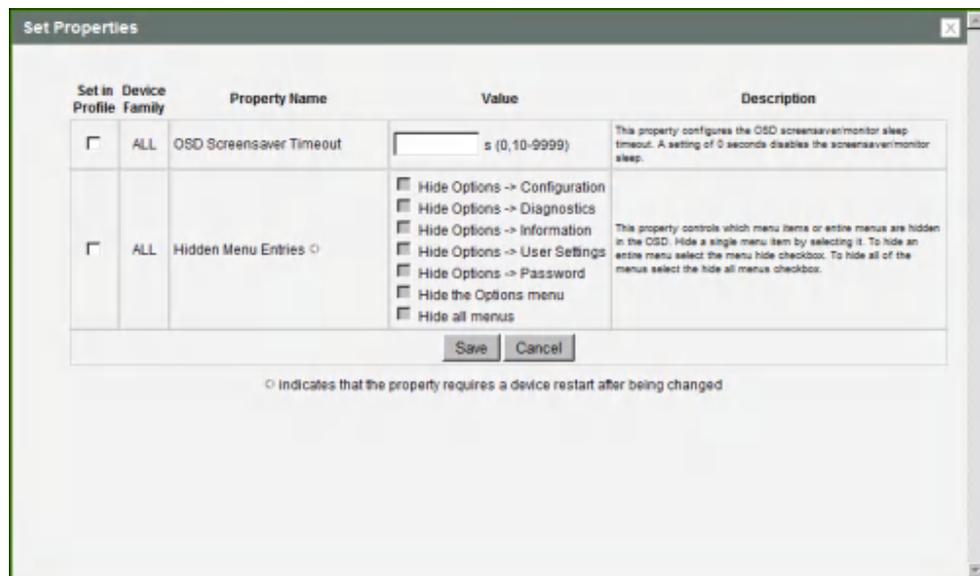


図 5-50 : MC OSD 設定

表 5-48 : MC 言語設定パラメータ

パラメータ	説明
OSD Screensaver Timeout	接続されたディスプレイが低電力モードに入るまでの秒数（10～9999）を使用して OSD スクリーンセーバタイムアウトを設定します。0 秒に設定すると、スクリーンセーバが無効になります。
Hidden Menu Entries	OSD ローカル GUI 上に表示しない項目を選択します。単一のメニュー項目、 Options メニュー全体、またはすべてのメニューを非表示にすることができます。 注意：このプロパティを変更した場合はデバイスを再起動する必要があります。

5.10.2 AWI クライアント : OSD 設定

このページの設定を使用すれば、ローカル OSD のモニタスクリーンセーバタイムアウトを設定することができます。このページは、**Configuration > OSD** メニューから表示することができます。

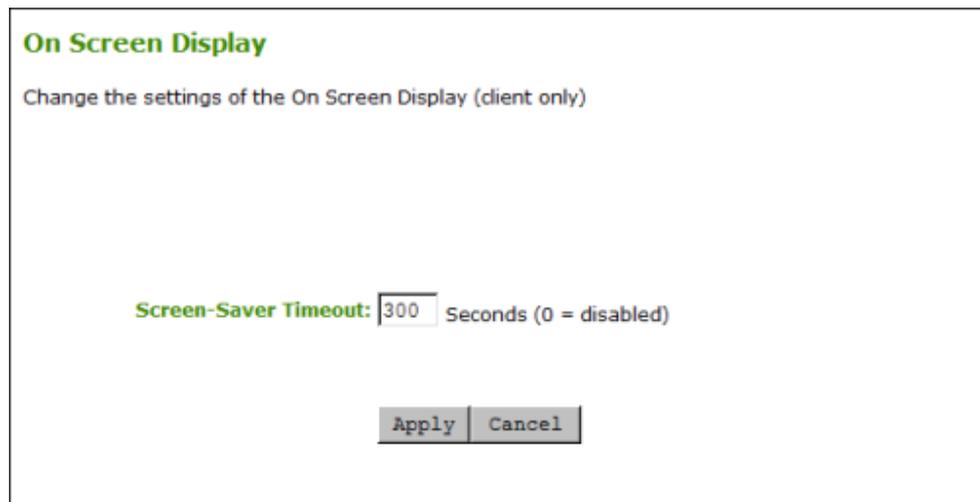


図 5-51 : AWI On Screen Display ページ

表 5-49 : AWI OSD パラメータ

パラメータ	説明
Screen-Saver Timeout	接続されたディスプレイが低電力モードに入るまでの秒数（10～9999）を使用して OSD スクリーンセーバタイムアウトを設定します。0 秒に設定すると、スクリーンセーバが無効になります。

5.10.3 OSD : OSD 設定

このページの設定を使用すれば、ローカル OSD のモニタスクリーンセーバタイムアウトを設定することができます。このページは、**Options > Configuration > OSD** メニューから表示することができます。

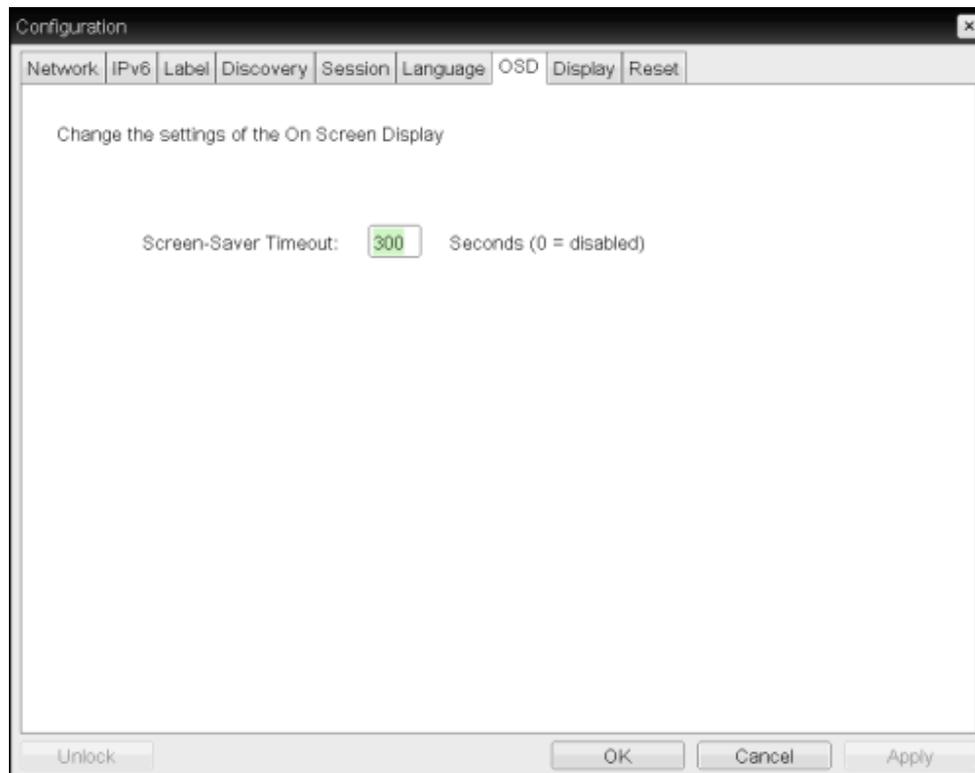


図 5-52 : OSD OSD ページ

表 5-50 : OSD OSD パラメータ

パラメータ	説明
Screen-Saver Timeout	接続されたディスプレイが低電力モードに入るまでの秒数（10～9999）を使用して OSD スクリーンセーバタイムアウトを設定します。0 秒に設定すると、スクリーンセーバが無効になります。

5.11 イメージ品質の設定

5.11.1 MC : イメージ設定

Image ページでは、PCoIP セッションのイメージ品質を変更するようにプロファイルを設定することができます。

注意 : この設定は、ゼロクライアントとホスト間のセッションにのみ適用されます。

MC でプロパティを有効にするには、**Set in Profile** チェックボックスをオンにし、指示に従ってフィールドを設定します。このページでプロパティを更新したら、**Save** をクリックして変更を保存します。

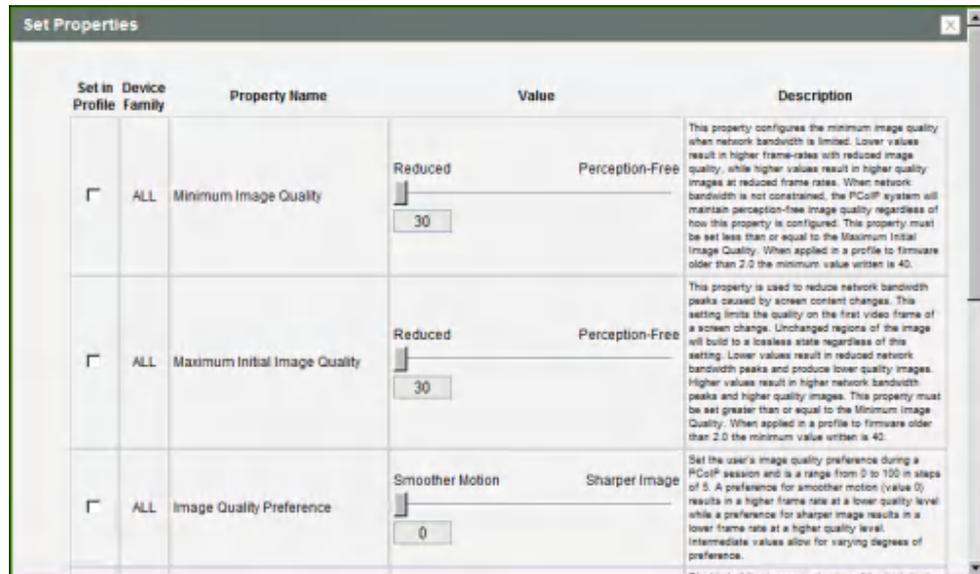


図 5-53 : MC イメージ設定

表 5-51 : MC イメージ設定パラメータ

パラメータ	説明
Minimum Image Quality	<p>ネットワーク帯域幅が制限されている場合にイメージ品質とフレームレートのバランスを取ることができます。ユースケースによっては、より高いフレームレートでより低い品質のイメージが必要な場合やより低いフレームレートでより高い品質のイメージが必要な場合があります。</p> <p>ネットワーク帯域幅が制限されている環境では、スライダを Reduced の方向に移動してより高いフレームレートを許可します。より高いイメージ品質を許可する場合は、スライダを Perception-Free の方向に移動します。ネットワーク帯域幅が制限されていない場合は、Minimum Image Quality パラメータに関係なく、PCoIP システムが問題のない品質を維持します。</p> <p>注意 : Maximum Initial Image Quality は Minimum Image Quality 以上にする必要があります。</p>
Maximum Initial Image Quality	<p>画面内容の変化に伴ってネットワーク帯域幅のピークを下げながら、より低い品質のイメージを生成する場合は、スライダを Reduced の方向に移動します。より高い品質のイメージを生成しながら、より高い帯域幅のピークも生成する場合は、スライダを Perception-Free の方向に移動します。</p> <p>このパラメータは、画面変化の最初の表示フレーム上の品質を制限します。イメージの無変化領域は、このパラメータに関係なく、ロスレス状態が維持されます。</p> <p>注意 : Maximum Initial Image Quality は Minimum Image Quality 以上にする必要があります。</p>

パラメータ	説明
Image Quality Preference	<p>より低い品質レベルでより高いフレームレートを生成する場合は、スライダを Smoother Motion の方向に移動します。より高い品質レベルでより低いフレームレートを生成する場合は、スライダを Sharper Image の方向に移動します。範囲は 0~100 の 5 段階です。</p> <p>注意：この設定は、5.0 以前のリリースを実行している VMware View 仮想デスクトップとの PCoIP セッションでは機能しません。</p>
Disable Build to Lossless	<p>イメージが完全なロスレス状態（つまり、ホストイメージソースと比較して理想的なピクセル単位レンダリング）になるまでバックグラウンドで再構築が継続される PCoIP プロトコルのロスレス構築機能を維持する場合は、このフィールドをオフのままにします。これはデフォルト（推奨）設定です。</p> <p>警告：Disable Build to Lossless フィールドをオンにすると、ゼロクライアントに表示されるイメージが劣化します。ユーザーが重要な機能を実行するために最適なイメージ品質を必要としないゼロクライアント管理者が判断した場合を除いて、このフィールドはオンにしないでください。この決定はゼロクライアント管理者独自の責任です。</p> <p>このフィールドをオンにした場合は、PCoIP プロトコルによって、クライアントイメージが知覚的にはロスレスだが、完全なロスレス状態ではない高品質イメージにすばやく構築されます。これにより、一部の帯域幅が節約されますが、イメージとデスクトップの内容を完全にロスレスにしなければならないユースケースにはお勧めできません。</p> <p>このフィールド設定に関する質問は、Teradici サポートにお問い合わせください。</p> <p>注意：この設定は、5.0 以前のリリースを実行している VMware View 仮想デスクトップとの PCoIP セッションでは機能しません。</p>
Enable Client Image Settings	<p>有効になっている場合は、クライアントのイメージ設定をセッションに使用するオプションがホストで使用可能になります。無効になっている場合は、ホストのイメージ設定が適用されます。</p> <p>注意：Image Quality Preference 設定にはこのルールが適用されません。</p>
Maximum Frame Rate	<p>最大フレームレートは、単一ネットワークリンク上での複数 PCoIP セッションの管理を容易にします。この設定によって、ユーザーが到達可能な上限が決定されます。フレーム制限なしにする場合は、このフィールドを 0 に設定します。値を設定すると、単一ユーザーがその値に制限されます。これにより、すべてのユーザーのユーザーエクスペリエンスの制御が容易になります。</p> <p>注意：この設定は、5.0 以前のリリースを実行している VMware View 仮想デスクトップとの PCoIP セッションでは機能しません。</p>

5.11.2 AWI ホスト : イメージ設定

Image ページでは、PCoIP セッションのイメージ品質を変更することができます。このページは、**Configuration > Image** メニューから表示することができます。

注意 : この設定は、ゼロクライアントとホスト間のセッションにのみ適用されます。

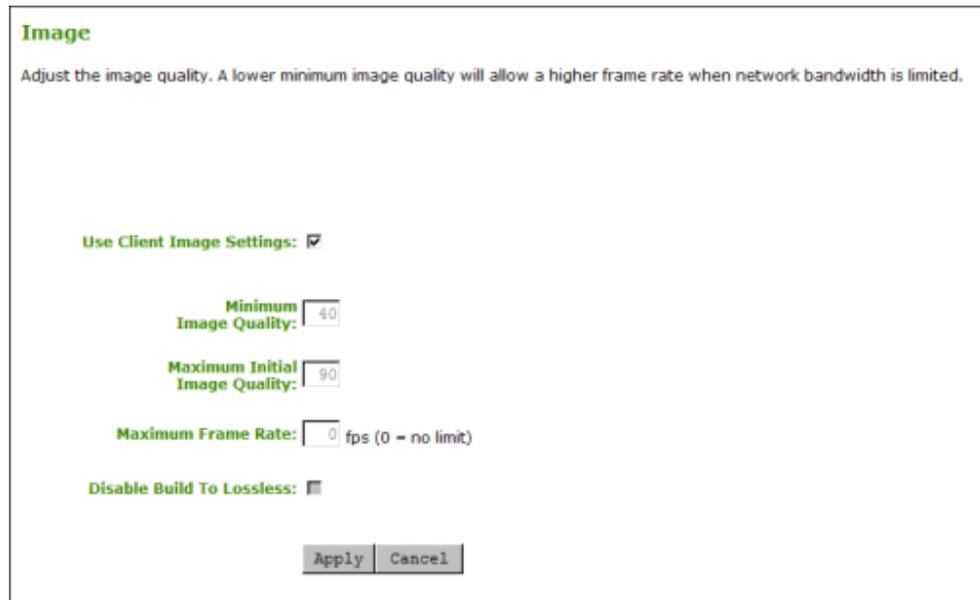


Image
Adjust the image quality. A lower minimum image quality will allow a higher frame rate when network bandwidth is limited.

Use Client Image Settings:

Minimum Image Quality:

Maximum Initial Image Quality:

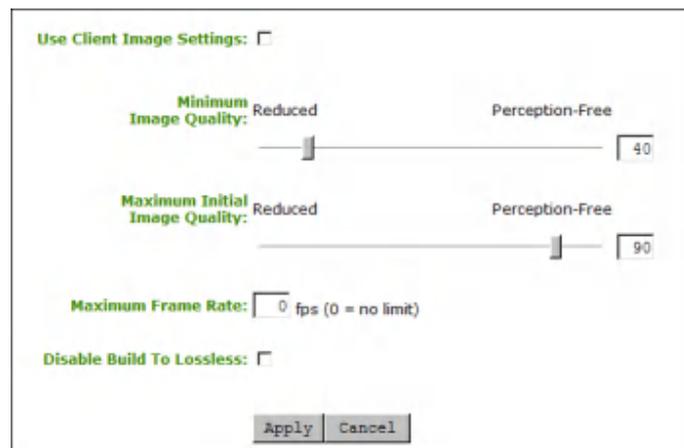
Maximum Frame Rate: fps (0 = no limit)

Disable Build To Lossless:

Apply Cancel

図 5-54 : AWI ホスト Image ページ

注意 : **Use Client Image Settings** フィールドが選択されていない場合は、下の図のように、このページのテキストボックスがスライダーに置き換えられます。



Use Client Image Settings:

Minimum Image Quality: Reduced Perception-Free

Maximum Initial Image Quality: Reduced Perception-Free

Maximum Frame Rate: fps (0 = no limit)

Disable Build To Lossless:

Apply Cancel

図 5-55 : AWI ホスト Image ページ – Use Client Image Settings が無効になっている場合

表 5-52 : AWI ホスト Image ページパラメータ

パラメータ	説明
-------	----

パラメータ	説明
Use Client Image Settings	<p>有効になっている場合は、このページのイメージ設定を編集することができません。表示される設定（グレーアウトされている）はホスト用としてフラッシュに保存されている設定です。</p> <p>無効になっている場合は、イメージ設定が編集可能になり、現在のセッションに適用されます。</p>
Minimum Image Quality	<p>ネットワーク帯域幅が制限されている場合にイメージ品質とフレームレートのバランスを取ることができます。ユースケースによっては、より高いフレームレートでより低い品質のイメージが必要な場合やより低いフレームレートでより高い品質のイメージが必要な場合があります。</p> <p>ネットワーク帯域幅が制限されている環境では、スライダを Reduced の方向に移動してより高いフレームレートを許可します。より高いイメージ品質を許可する場合は、スライダを Perception-Free の方向に移動します。ネットワーク帯域幅が制限されていない場合は、Minimum Image Quality パラメータに関係なく、PCoIP システムが問題のない品質を維持します。</p> <p>注意：Maximum Initial Image Quality は Minimum Image Quality 以上にする必要があります。</p>
Maximum Initial Image Quality	<p>画面内容の変化に伴ってネットワーク帯域幅のピークを下げながら、より低い品質のイメージを生成する場合は、スライダを Reduced の方向に移動します。より高い品質のイメージを生成しながら、より高い帯域幅のピークも生成する場合は、スライダを Perception-Free の方向に移動します。</p> <p>このパラメータは、画面変化の最初の表示フレーム上の品質を制限します。イメージの無変化領域は、このパラメータに関係なく、ロスレス状態が維持されます。</p> <p>注意：Maximum Initial Image Quality は Minimum Image Quality 以上にする必要があります。</p>
Image Quality Preference	<p>より低い品質レベルでより高いフレームレートを生成する場合は、スライダを Smoother Motion の方向に移動します。より高い品質レベルでより低いフレームレートを生成する場合は、スライダを Sharper Image の方向に移動します。範囲は 0～100 の 5 段階です。</p> <p>注意：この設定は、5.0 以前のリリースを実行している VMware View 仮想デスクトップとの PCoIP セッションでは機能しません。</p>
Maximum Frame Rate	<p>最大フレームレートは、単一ネットワークリンク上での複数 PCoIP セッションの管理を容易にします。この設定によって、ユーザが到達可能な上限が決定されます。フレーム制限なしにする場合は、このフィールドを 0 に設定します。値を設定すると、単一ユーザがその値に制限されます。これにより、すべてのユーザのユーザエクスペリエンスの制御が容易になります。</p> <p>注意：この設定は、5.0 以前のリリースを実行している VMware View</p>

パラメータ	説明
	仮想デスクトップとの PCoIP セッションでは機能しません。
Disable Build to Lossless	<p>イメージが完全なロスレス状態（つまり、ホストイメージソースと比較して理想的なピクセル単位レンダリング）になるまでバックグラウンドで再構築が継続される PCoIP プロトコルのロスレス構築機能を維持する場合は、このフィールドをオフのままにします。これはデフォルト（推奨）設定です。</p> <p>警告：Disable Build to Lossless フィールドをオンにすると、ゼロクライアントに表示されるイメージが劣化します。ユーザが重要な機能を実行するために最適なイメージ品質を必要としていないとゼロクライアント管理者が判断した場合を除いて、このフィールドはオンにしないでください。この決定はゼロクライアント管理者独自の責任です。</p> <p>このフィールドをオンにした場合は、PCoIP プロトコルによって、クライアントイメージが知覚的にはロスレスだが、完全なロスレス状態ではない高品質イメージにすばやく構築されます。これにより、一部の帯域幅が節約されますが、イメージとデスクトップの内容を完全にロスレスにしなければならないユースケースにはお勧めできません。</p> <p>このフィールド設定に関する質問は、Teradici サポートにお問い合わせください。</p> <p>注意：この設定は、5.0 以前のリリースを実行している VMware View 仮想デスクトップとの PCoIP セッションでは機能しません。</p>

5.11.3 AWI クライアント：イメージ設定

Image ページでは、PCoIP セッションのイメージ品質を変更することができます。このページは、**Configuration > Image** メニューから表示することができます。

注意：この設定は、ゼロクライアントとホスト間のセッションにのみ適用されます。

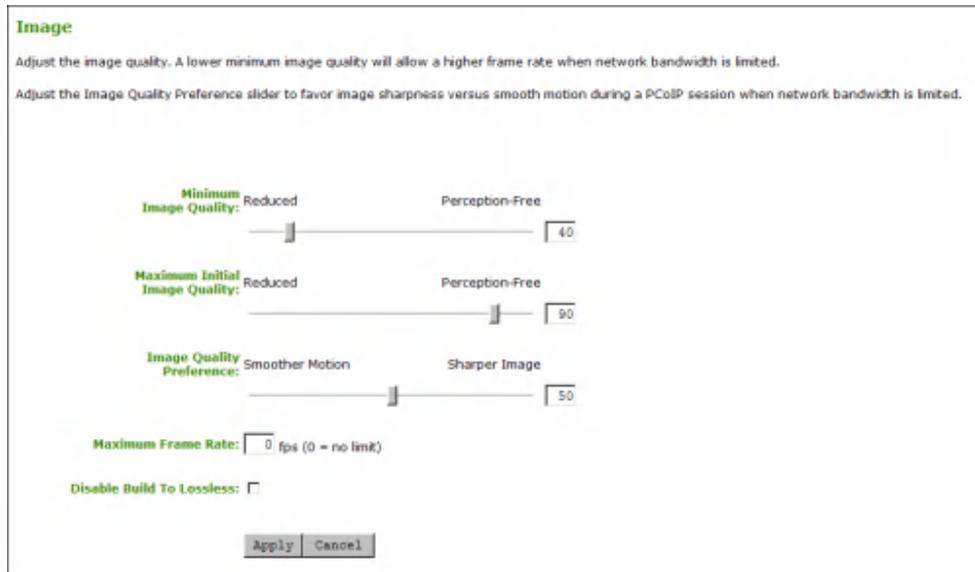


図 5-56 : AWI クライアント Image ページ

表 5-53 : AWI クライアント Image ページパラメータ

パラメータ	説明
Minimum Image Quality	<p>ネットワーク帯域幅が制限されている場合にイメージ品質とフレームレートのバランスを取ることができます。ユースケースによっては、より高いフレームレートでより低い品質のイメージが必要な場合やより低いフレームレートでより高い品質のイメージが必要な場合があります。</p> <p>ネットワーク帯域幅が制限されている環境では、スライダを Reduced の方向に移動してより高いフレームレートを許可します。より高いイメージ品質を許可する場合は、スライダを Perception-Free の方向に移動します。ネットワーク帯域幅が制限されていない場合は、Minimum Image Quality パラメータに関係なく、PCoIP システムが問題のない品質を維持します。</p> <p>注意 : Maximum Initial Image Quality は Minimum Image Quality 以上にする必要があります。</p>
Maximum Initial Image Quality	<p>画面内容の変化に伴ってネットワーク帯域幅のピークを下げながら、より低い品質のイメージを生成する場合は、スライダを Reduced の方向に移動します。より高い品質のイメージを生成しながら、より高い帯域幅のピークも生成する場合は、スライダを Perception-Free の方向に移動します。</p> <p>このパラメータは、画面変化の最初の表示フレーム上の品質を制限します。イメージの無変化領域は、このパラメータに関係なく、ロスレス状態が維持されます。</p> <p>注意 : Maximum Initial Image Quality は Minimum Image Quality 以上にする必要があります。</p>

パラメータ	説明
Image Quality Preference	<p>より低い品質レベルでより高いフレームレートを生成する場合は、スライダを Smoother Motion の方向に移動します。より高い品質レベルでより低いフレームレートを生成する場合は、スライダを Sharper Image の方向に移動します。範囲は 0~100 の 5 段階です。</p> <p>注意：この設定は、5.0 以前のリリースを実行している VMware View 仮想デスクトップとの PCoIP セッションでは機能しません。</p>
Maximum Frame Rate	<p>最大フレームレートは、単一ネットワークリンク上での複数 PCoIP セッションの管理を容易にします。この設定によって、ユーザが到達可能な上限が決定されます。フレーム制限なしにする場合は、このフィールドを 0 に設定します。値を設定すると、単一ユーザがその値に制限されます。これにより、すべてのユーザのユーザエクスペリエンスの制御が容易になります。</p> <p>注意：この設定は、5.0 以前のリリースを実行している VMware View 仮想デスクトップとの PCoIP セッションでは機能しません。</p>
Disable Build to Lossless	<p>イメージが完全なロスレス状態（つまり、ホストイメージソースと比較して理想的なピクセル単位レンダリング）になるまでバックグラウンドで再構築が継続される PCoIP プロトコルのロスレス構築機能を維持する場合は、このフィールドをオフのままにします。これはデフォルト（推奨）設定です。</p> <p>警告：Disable Build to Lossless フィールドをオンにすると、ゼロクライアントに表示されるイメージが劣化します。ユーザが重要な機能を実行するために最適なイメージ品質を必要としないゼロクライアント管理者が判断した場合を除いて、このフィールドはオンにしないでください。この決定はゼロクライアント管理者独自の責任です。</p> <p>このフィールドをオンにした場合は、PCoIP プロトコルによって、クライアントイメージが知覚的にはロスレスだが、完全なロスレス状態ではない高品質イメージにすばやく構築されます。これにより、一部の帯域幅が節約されますが、イメージとデスクトップの内容を完全にロスレスにしなければならないユースケースにはお勧めできません。このフィールド設定に関する質問は、Teradici サポート にお問い合わせください。</p> <p>注意：この設定は、5.0 以前のリリースを実行している VMware View 仮想デスクトップとの PCoIP セッションでは機能しません。</p>

5.11.4 OSD：イメージ設定

Image ページでは、PCoIP セッションのイメージ品質を変更することができます。このページは、**Options > User Settings > Image** メニューから表示することができます。

注意：この設定は、ゼロクライアントとホスト間のセッションにのみ適用されます。



図 5-57 : OSD Image ページ

注意 : OSD では、このページに **Options->User Settings** メニューからアクセスすることができます。

表 5-54 : OSD Image ページパラメータ

パラメータ	説明
Image Quality Preference	<p>より低い品質レベルでより高いフレームレートを生成する場合は、スライダを Smoother Motion の方向に移動します。より高い品質レベルでより低いフレームレートを生成する場合は、スライダを Sharper Image の方向に移動します。範囲は 0~100 の 5 段階です。</p> <p>注意 : この設定は、5.0 以前のリリースを実行している VMware View 仮想デスクトップとの PCoIP セッションでは機能しません。</p>

5.12 モニタエミュレーションの設定

5.12.1 MC : モニタエミュレーション

Monitor Emulation ページでは、モニタエミュレーション機能を有効または無効にするようにプロファイルを設定することができます。このページは、未だにモニタエミュレーションを使用しているホストカード上でのみ使用することができます。クライアント上では無効になっているため、編集することができません。

ディスプレイが接続されていないと起動しない PC やワークステーションがあります。モニタエミュレーションは、起動プロセスの完了を保証する汎用表示を提供します。セッションが確立されると、クライアントのディスプレイ情報がホストに送信されます。

MC でプロパティを有効にするには、**Set in Profile** チェックボックスをオンにし、指示に従ってフィールドを設定します。このページでプロパティを更新したら、**Save** をクリックして変更を保存します。

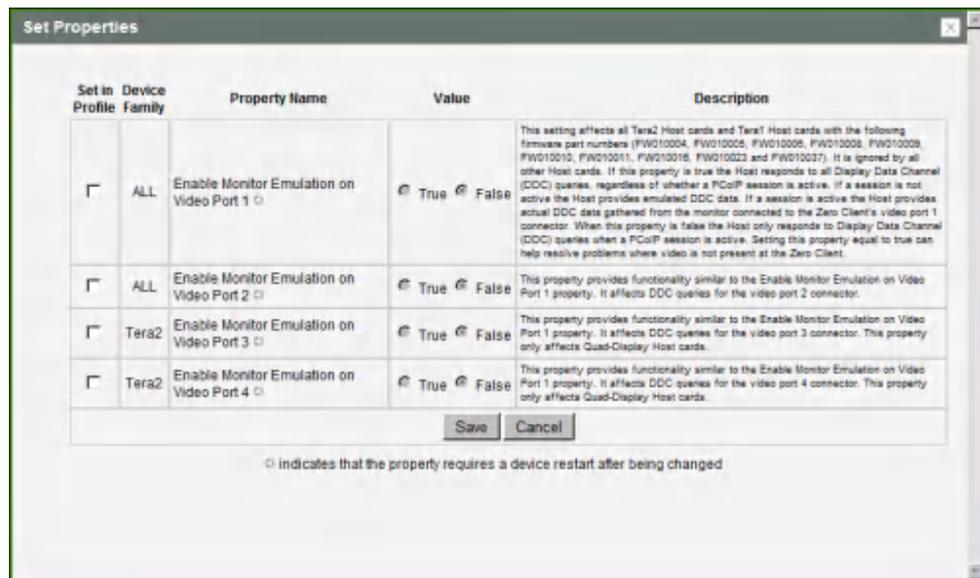


図 5-58 : MC Monitor Emulation ページ

表 5-55 : MC モニタパラメータ

パラメータ	説明
Enable Monitor Emulation on Video Port 1	有効になっている場合は、PCoIPセッションがアクティブかどうかに関係なく、ホストがすべてのディスプレイデータチャネル (DDC) の問い合わせに応答します。セッションがアクティブでない場合は、ホストがエミュレートした DDC データを提供します。セッションがアクティブな場合は、ホストがクライアントのポート 1 コネクタに接続されたモニタから収集した実際の DDC データを提供します。 無効になっている場合は、PCoIPセッションがアクティブなときの

パラメータ	説明
	<p>み、ホストがディスプレイデータチャンネル（DDC）の問い合わせに応答します。</p> <p>注意：このフィールドを有効にすると、クライアントでビデオが表示されない問題の解決が支援される場合があります。</p> <p>注意：このプロパティを変更した場合はデバイスを再起動する必要があります。</p>
Enable Monitor Emulation on Video Port 2	<p>このフィールドは、ポート 2 コネクタに対する DDC 問い合わせに影響を与え、ポート 1 コネクタの場合と同等の機能を提供します。</p> <p>注意：このプロパティを変更した場合はデバイスを再起動する必要があります。</p>
Enable Monitor Emulation on Video Port 3	<p>このフィールドは、ポート 3 コネクタに対する DDC 問い合わせに影響を与え、ポート 1 コネクタの場合と同等の機能を提供します。</p> <p>注意：このプロパティを変更した場合はデバイスを再起動する必要があります。</p>
Enable Monitor Emulation on Video Port 4	<p>このフィールドは、ポート 4 コネクタに対する DDC 問い合わせに影響を与え、ポート 1 コネクタの場合と同等の機能を提供します。</p> <p>注意：このプロパティを変更した場合はデバイスを再起動する必要があります。</p>

5.12.2 AWI Tera1 ホスト：モニタエミュレーション

Monitor Emulation ページでは、モニタエミュレーション機能を有効または無効にすることができます。このページは、未だにモニタエミュレーションを使用しているホストカード上でのみ使用することができます。クライアント上では無効になっているため、編集することができません。

ディスプレイが接続されていないと起動しない PC やワークステーションがあります。モニタエミュレーションは、起動プロセスの完了を保証する汎用表示を提供します。セッションが確立されると、クライアントのディスプレイ情報がホストに送信されます。

このページは、**Configuration > Monitor Emulation** メニューから表示することができます。

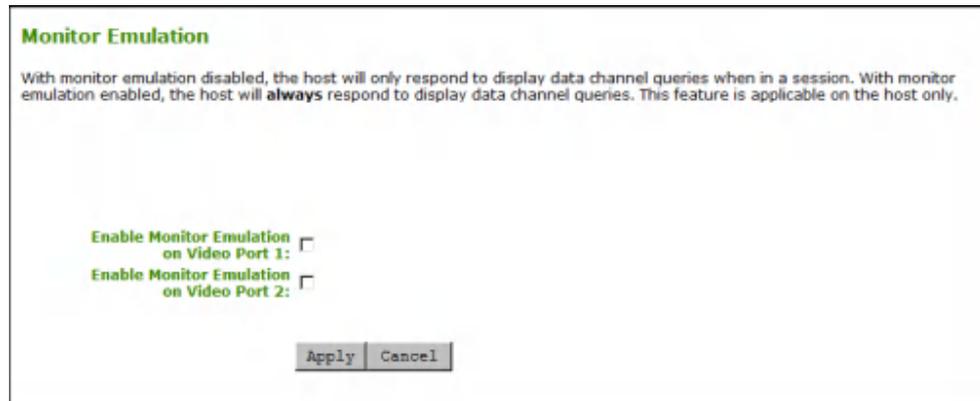


図 5-59 : AWI Tera1 ホスト Monitor Emulation ページ

表 5-56 : AWI Tera1 ホストモニタパラメータ

パラメータ	説明
Enable Monitor Emulation on DVI-1	<p>有効になっている場合は、PCoIPセッションがアクティブかどうかに関係なく、ホストがすべてのディスプレイデータチャンネル（DDC）の問い合わせに応答します。セッションがアクティブでない場合は、ホストがエミュレートした DDC データを提供します。セッションがアクティブな場合は、ホストがクライアントのポート 1 コネクタに接続されたモニタから収集した実際の DDC データを提供します。</p> <p>無効になっている場合は、PCoIPセッションがアクティブなときのみ、ホストがディスプレイデータチャンネル（DDC）の問い合わせに応答します。</p> <p>注意：このフィールドを有効にすると、クライアントでビデオが表示されない問題の解決が支援される場合があります。</p>
Enable Monitor Emulation on DVI-2	<p>このフィールドは、ポート 2 コネクタに対する DDC 問い合わせに影響を与え、ポート 1 コネクタの場合と同等の機能を提供します。</p>

5.12.3 AWI Tera2 ホスト：モニタエミュレーション

Monitor Emulation ページでは、モニタエミュレーション機能を有効または無効にすることができます。このページは、モニタエミュレーションを使用しているホストカード上でのみ使用することができます。クライアント上では無効になっているため、編集することができません。

ディスプレイが接続されていないと起動しない PC やワークステーションがあります。モニタエミュレーションは、起動プロセスの完了を保証する汎用表示を提供します。セッションが確立されると、クライアントのディスプレイ情報がホストに送信されます。

このページは、**Configuration > Monitor Emulation** メニューから表示することができます。

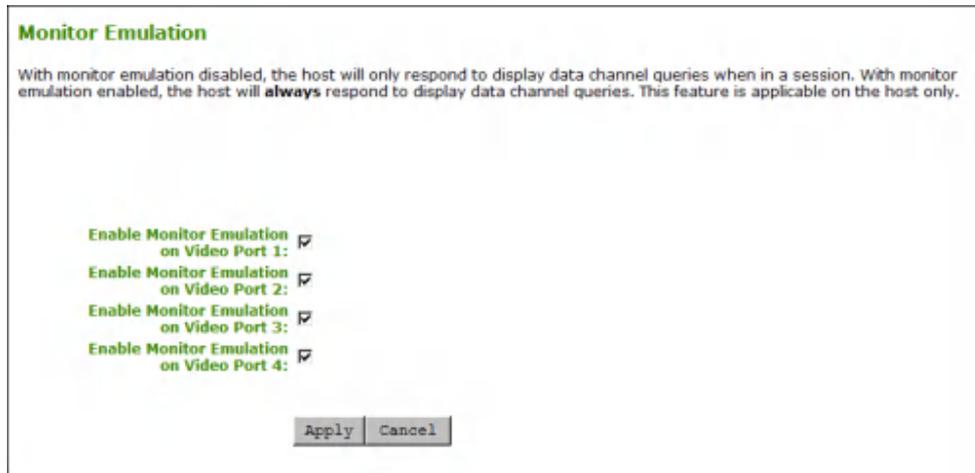


図 5-60 : AWI Tera2 ホスト Monitor Emulation ページ

表 5-57 : AWI Tera2 ホストモニタパラメータ

パラメータ	説明
Enable Monitor Emulation on Video Port 1	<p>有効になっている場合は、PCoIPセッションがアクティブかどうかに関係なく、ホストがすべてのディスプレイデータチャンネル（DDC）の問い合わせに応答します。セッションがアクティブでない場合は、ホストがエミュレートした DDC データを提供します。セッションがアクティブな場合は、ホストがクライアントのポート 1 コネクタに接続されたモニタから収集した実際の DDC データを提供します。</p> <p>無効になっている場合は、PCoIPセッションがアクティブなときのみ、ホストがディスプレイデータチャンネル（DDC）の問い合わせに応答します。</p> <p>注意：このフィールドを有効にすると、クライアントでビデオが表示されない問題の解決が支援される場合があります。</p>
Enable Monitor Emulation on Video Port 2	このフィールドは、ポート 2 コネクタに対する DDC 問い合わせに影響を与え、ポート 1 コネクタの場合と同等の機能を提供します。
Enable Monitor Emulation on Video Port 3	このフィールドは、ポート 3 コネクタに対する DDC 問い合わせに影響を与え、ポート 1 コネクタの場合と同等の機能を提供します。
Enable Monitor Emulation on Video Port 4	このフィールドは、ポート 4 コネクタに対する DDC 問い合わせに影響を与え、ポート 1 コネクタの場合と同等の機能を提供します。

5.13 時間の設定

5.13.1 MC : 時間設定

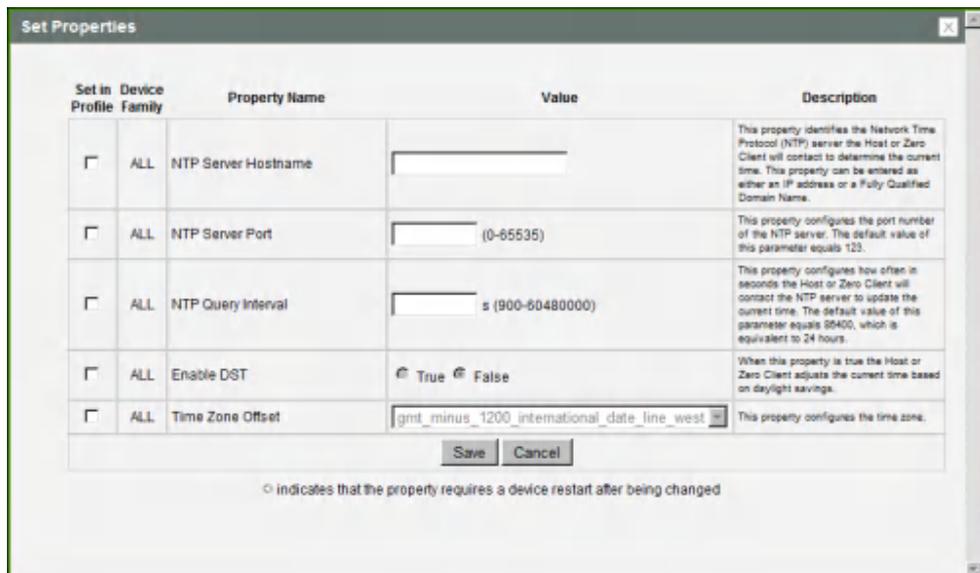
Time ページでは、ネットワークタイムプロトコル (NTP) パラメータを使用して、ホストとクライアントのイベントログに NTP 時間に基づくタイムスタンプを付けられるようにプロファイルを設定することができます。

注意：クライアントが DHCP 用に設定され、DHCP サーバが NTP サーバアドレスを提供している場合は、このアドレスが手動で設定されたものの NTP サーバよりも優先されます。また、NTP が無効になっている場合は、有効になります。

注意：クライアントは NTP サーバからタイムゾーンまたは夏時間 (DST) 情報を取得しません。

注意：システムトラブルシューティングを容易にするために、ユーザがユーザイベントと診断イベントログのエントリを対応付けることができるように NTP パラメータを設定します。

MC でプロパティを有効にするには、**Set in Profile** チェックボックスをオンにし、指示に従ってフィールドを設定します。このページでプロパティを更新したら、**Save** をクリックして変更を保存します。



Set in Profile	Device Family	Property Name	Value	Description
<input type="checkbox"/>	ALL	NTP Server Hostname	<input type="text"/>	This property identifies the Network Time Protocol (NTP) server the Host or Zero Client will contact to determine the current time. This property can be entered as either an IP address or a Fully Qualified Domain Name.
<input type="checkbox"/>	ALL	NTP Server Port	<input type="text"/> (0-65535)	This property configures the port number of the NTP server. The default value of this parameter equals 123.
<input type="checkbox"/>	ALL	NTP Query Interval	<input type="text"/> s (900-60480000)	This property configures how often in seconds the Host or Zero Client will contact the NTP server to update the current time. The default value of this parameter equals 60400, which is equivalent to 24 hours.
<input type="checkbox"/>	ALL	Enable DST	<input checked="" type="radio"/> True <input type="radio"/> False	When this property is true the Host or Zero Client adjusts the current time based on daylight savings.
<input type="checkbox"/>	ALL	Time Zone Offset	<input type="text"/> gmst_minus_1200_international_date_line_west	This property configures the time zone.

○ indicates that the property requires a device restart after being changed

図 5-61 : MC 時間設定

表 5-58 : MC 時間設定パラメータ

パラメータ	説明
NTP Server Hostname	ホストまたはクライアントが現在時刻を決定するために接触する NTP サーバの IP アドレスまたは完全修飾ドメイン名 (FQDN) を設定します。

パラメータ	説明
NTP Server Port	NTP サーバのポート番号を設定します。デフォルトの NTP サーバポート値は 123 です。
NTP Query Interval	ホストまたはクライアントが現在時刻を更新するために NTP サーバに接触する頻度（秒単位）を設定します。デフォルトの問い合わせ間隔は、86400 秒、つまり、24 時間です。
Enable DST	夏時間（DST）の自動調節を有効または無効にします。
Time Zone Offset	必要なタイムゾーンを選択します。

5.13.2 AWI : 時間設定

Time ページでは、ホストとクライアントのイベントログに NTP 時間に基づくタイムスタンプを付けられるようにネットワークタイムプロトコル（NTP）パラメータを設定することができます。

注意：クライアントが DHCP 用に設定され、DHCP サーバが NTP サーバアドレスを提供している場合は、このアドレスが手動で設定されたどの NTP サーバよりも優先されます。また、NTP が無効になっている場合は、有効になります。

注意：クライアントは NTP サーバからタイムゾーンまたは夏時間（DST）情報を取得しません。

注意：システムトラブルシューティングを容易にするために、ユーザがユーザイベントと診断イベントログのエントリを対応付けることができるように NTP パラメータを設定します。

このページは、ホストまたはクライアントの **Configuration > Time** メニューから表示することができます。

Time
Change the local time configuration

Current time: 08/21/2012 13:22:29

Enable NTP:

Identify NTP Host by: IP address FQDN

NTP Host DNS Name:

NTP Host Port:

NTP Query Interval: Day(s)

Time Zone:

Enable Daylight Saving Time:

Apply Cancel

図 5-62 : AWI Time ページ

表 5-59 : AWI Time ページパラメータ

パラメータ	説明
Current Time	NTP に基づく時間が表示されます。
Enable NTP	NTP 機能を有効または無効にします。
Identify NTP Host by	NTP ホストを IP アドレスで識別するか、完全修飾ドメイン名 (FQDN) で識別するかを選択します。NTP が無効になっている場合は、このフィールドが不要なため、編集不可になります。無効な IP アドレスまたは DNS 名を入力した場合は、その修正を促すメッセージが表示されます。パラメータは選択した方式によって異なります。 <ul style="list-style-type: none"> • IP Address : NTP ホストの IP アドレスを示します。 • FQDN : NTP ホストの DNS 名を示します。
NTP Host Port	NTP サーバのポート番号を設定します。デフォルトの NTP サーバポート値は 123 です。
NTP Query Interval	問い合わせ間隔を設定します。1 つ目のフィールドが時間間隔用で、2 つ目のフィールドが時間単位 (分、時間、日、または週) 用です。
Time Zone	ローカルタイムゾーンを選択します。
Enable Daylight Savings	夏時間 (DST) の自動調節を有効または無効にします。

パラメータ	説明
Time	

5.14 セキュリティの設定

5.14.1 MC : セキュリティ設定

このページの設定を使用すれば、ホストとクライアントに使用されるセキュリティパラメータでプロファイルを構成することができます。

MCでプロパティを有効にするには、**Set in Profile** チェックボックスをオンにし、指示に従ってフィールドを設定します。このページでプロパティを更新したら、**Save** をクリックして変更を保存します。

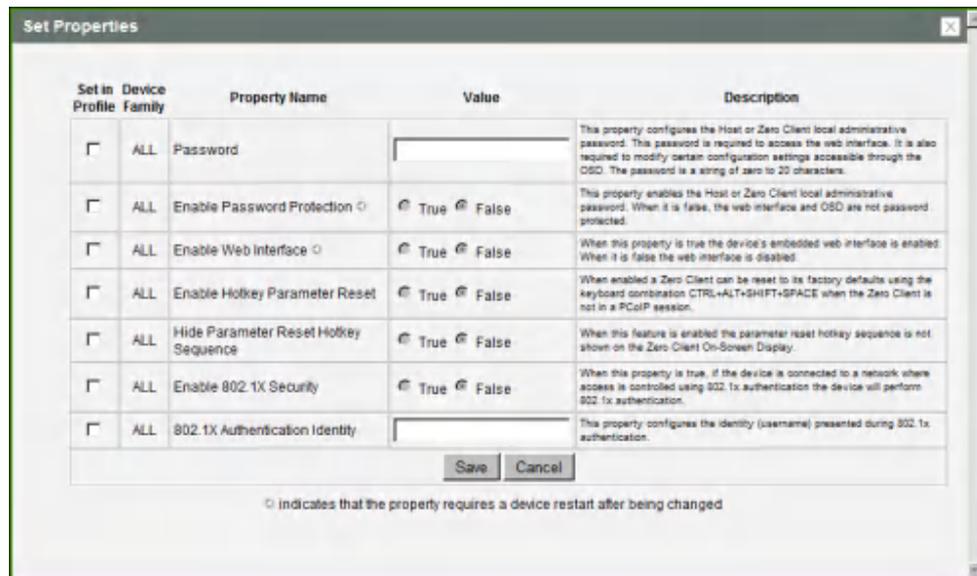


図 5-63 : MCセキュリティ設定

表 5-60 : MCセキュリティ設定パラメータ

パラメータ	説明
Password	ホストまたはクライアントの管理用ウェブインターフェース (AWI) のパスワードを入力します。このパスワードは、クライアントのオンスクリーンディスプレイ (OSD) 経由でアクセス可能な特定の構成設定を変更する場合にも必要です。 このフィールドには 0~20 文字を入力することができます。
Enable Password Protection	有効になっている場合は、ホストまたはクライアントの AWI パスワードが必要です。無効になっている場合は、AWI と OSD がパスワードで保護されません。

パラメータ	説明
Enable Web Interface	有効になっている場合は、ホストまたはクライアントの AWI が有効になります。無効になっている場合は、AWI が無効になります。
Enable Hotkey Parameter Reset	有効になっている場合は、クライアントが PCoIP セッションに入っていないときに、キーボードの組み合わせの Ctrl+Alt+Shift+Space を使用してクライアントを工場出荷時設定にリセットすることができます。
Hide Parameter Reset Hotkey Sequence	有効になっている場合は、リセットホットキーシーケンスがクライアント OSD 上に表示されません。
Enable 802.1X Security	有効になっている場合は、デバイスが、802.1X 認証を通してアクセスが管理されたネットワークに接続されている場合に 802.1X 認証を実行します。
802.1X Authentication Identity	802.1X 認証で提示するためのユーザ名を設定します。

5.14.2 AWI : セキュリティ設定に関するヘルプ

AWI のセキュリティ設定は、AWI の [Network Settings](#) ページ (**Configuration > Network** メニューからアクセス) に配置されています。このページの以下のフィールドに関する説明を参照してください。

- Enable 802.1X Security
- Authentication
- Identity
- Client Certificate

5.15 オーディオ承認の設定

5.15.1 MC : オーディオ承認

このページの設定を使用すれば、ホストとクライアントに使用されるオーディオパラメータでプロファイルを構成することができます。

MC でプロパティを有効にするには、**Set in Profile** チェックボックスをオンにし、指示に従ってフィールドを設定します。このページでプロパティを更新したら、**Save** をクリックして変更を保存します。

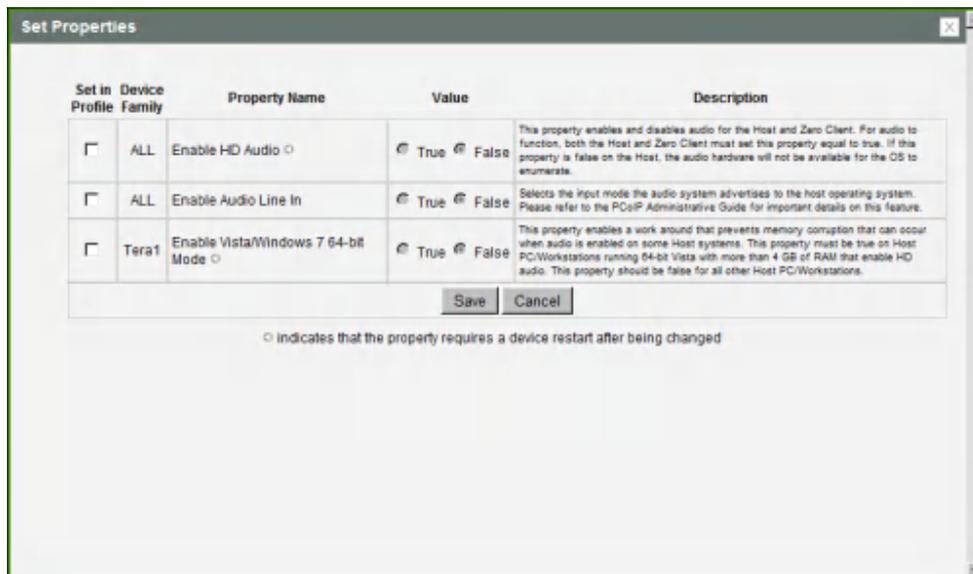


図 5-64 : MC オーディオ承認

表 5-61 : MC オーディオ承認パラメータ

パラメータ	説明
Enable HD Audio	<p>デバイス上でオーディオサポートを設定できるようにします。</p> <p>注意：このプロパティはホストとクライアントの両方で有効にする必要があります。</p> <p>無効になっている場合は、ホストオペレーティングシステムのエミュレートにオーディオハードウェアを使用することができません。</p> <p>注意：このプロパティを変更した場合はデバイスを再起動する必要があります。</p>
Enable Audio Line In	<p>このプロパティによって、オーディオシステムからホストオペレーティングシステムにアダプタイズされる入力モードが決定されます。有効になっている場合は、クライアント上で発見されたライン入力コネクタが標準のライン入力として使用されます。無効になっている場合は、クライアント上で発見されたライン入力コネクタがマイクロホン入力として使用されます。</p>
Enable Microsoft Windows Vista 64-bit Mode	<p>Windows Vista 64 ビットバージョンと Windows 7 64 ビットバージョンのオペレーティングシステムの場合にこのオプションを有効にします。</p> <p>警告：Windows XP 64 または 32 ビットオペレーティングシステムではこのモードを使用しないでください。</p> <p>Linux 64 ビットオペレーティングシステムの場合は、64 ビットモードを有効にする必要がありません。Linux カーネルは最新の PCoIP オーディオ CODEC サポートを使用してコンパイルする必要があります。</p> <p>注意：このプロパティを変更した場合はデバイスを再起動する必要があります。</p>

5.15.2 AWI Tera1 ホスト : オーディオ承認

最初のセッションを開始するときに、[Initial Setup](#) ページでオーディオ承認を設定することができます。

それ以降のセッションでは、**Audio** ページ (**Permissions** > **Audio** メニューからアクセス) を使用して、デバイスのオーディオ承認を設定します。このページでオプションを更新したら、**Apply** をクリックして変更を保存します。

管理用ウェブインターフェースで **Audio** ページを表示するには、**Permissions** メニューを選択してから、**Audio** をクリックします。



図 5-65 : AWI Tera1 ホスト Audio ページ

表 5-62 : AWI Tera1 ホスト Audio ページパラメータ

パラメータ	説明
Enable HD Audio	デバイス上でオーディオサポートを設定できるようにします。 注意：このプロパティはホストとクライアントの両方で有効にする必要があります。 無効になっている場合は、ホストオペレーティングシステムのエミュレートにオーディオハードウェアを使用することができません。
Enable Microsoft® Windows Vista® / Windows® 7 64-bit Mode	Windows Vista 64 ビットバージョンと Windows 7 64 ビットバージョンのオペレーティングシステムの場合にこのオプションを有効にします。 警告：Windows XP 64 または 32 ビットオペレーティングシステムではこのモードを使用しないでください。 Linux 64 ビットオペレーティングシステムの場合は、64 ビットモードを有効にする必要がありません。Linux カーネルは最新の PCoIP オーディオ CODEC サポートを使用してコンパイルする必要があります。
Enable Audio Line In	このプロパティによって、オーディオシステムからホストオペレーティングシステムにアダプタイズされる入力モードが決定されます。有効になっている

パラメータ	説明
	<p>る場合は、クライアント上で発見されたライン入力コネクタが標準のライン入力として使用されます。無効になっている場合は、クライアント上で発見されたライン入力コネクタがマイクロホン入力として使用されます。</p> <p>注意：デバイス上に Windows Vista または Windows 7 がインストールされている場合は、画面上の指示に従ってください。</p>

5.15.3 AWI クライアント：オーディオ承認

最初のセッションを開始するときに、[Initial Setup](#) ページでオーディオ承認を設定することができます。

それ以降のセッションでは、**Audio** ページ (**Permissions > Audio** メニューからアクセス) を使用して、デバイスのオーディオ承認を設定します。このページでオプションを更新したら、**Apply** をクリックして変更を保存します。

管理用ウェブインターフェースで **Audio** ページを表示するには、**Permissions** メニューを選択してから、**Audio** をクリックします。

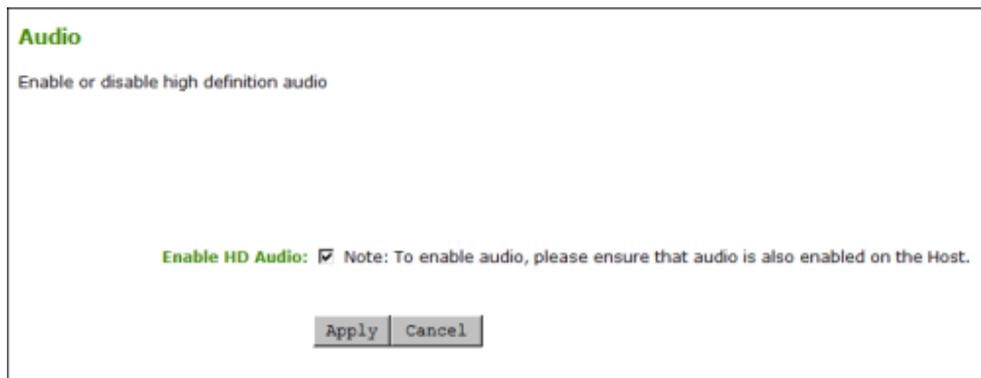


図 5-66 : AWI クライアント **Audio** ページ

表 5-63 : AWI クライアント **Audio** ページパラメータ

パラメータ	説明
Enable HD Audio	<p>デバイス上でオーディオサポートを設定できるようにします。</p> <p>注意：このプロパティはホストとクライアントの両方で有効にする必要があります。</p> <p>無効になっている場合は、ホストオペレーティングシステムのエミュレートにオーディオハードウェアを使用することができません。</p>

5.16 電源承認の設定

5.16.1 MC : 電源承認

このページの設定を使用すれば、ホストとクライアントの電源承認でプロファイルを構成することができます。

MC でプロパティを有効にするには、**Set in Profile** チェックボックスをオンにし、指示に従ってフィールドを設定します。このページでプロパティを更新したら、**Save** をクリックして変更を保存します。

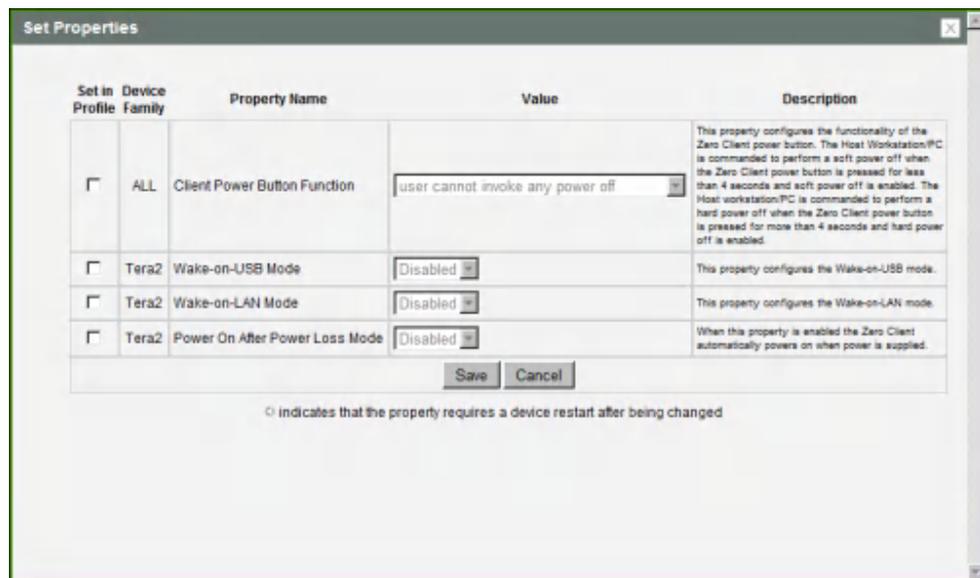


図 5-67 : MC 電源承認

表 5-64 : MC 電源承認パラメータ

パラメータ	説明
Client Power Button Function	<p>このプロパティによって、クライアントのリモート PC ボタンの機能が設定されます。</p> <p>ホストは、クライアントのリモート PC ボタンの押下が 4 秒未満で、ソフト電源オフが有効になっている場合に、ソフト電源オフを実行（つまり、スリープモードに移行）するように指示されます。</p> <p>ホストは、クライアントのリモート PC ボタンの押下が 4 秒以上で、ハード電源オフが有効になっている場合に、ハード電源オフ（つまり、シャットダウン）を実行するように指示されます。</p> <p>以下のオプションの中から選択します。</p> <ul style="list-style-type: none"> • user cannot invoke any power off : ユーザはホストをシャットダウンしたり、ホストをスリープモードに移行したりすることができません。 • user can only invoke a hard power off : ユーザはホストをシャットダウンすることはできますが、ホストをスリープモードに移行することはできません。

パラメータ	説明
	<ul style="list-style-type: none"> • user can only invoke a soft power off : ユーザはホストをスリープモードに移行することはできますが、ホストをシャットダウンすることはできません。 • user can invoke soft and hard power offs : ユーザはホストをスリープモードに移行することも、ホストをシャットダウンすることもできます。
Wake-on-USB Mode	有効になっている場合は、ユーザがマウスを移動したとき、または、キーボード上のキーを押したときにスリープモードから再開するようにホストが設定されます。
Wake-on-LAN Mode	有効になっている場合は、ユーザがクライアントの Remote PC ボタンを押したとき、または、 Connect ウィンドウの Connect ボタンをクリックしたときに、スリープモードから再開するようにホストが設定されます。
Power On After Power Loss Mode	有効になっている場合は、クライアントが、電源が供給された時点で自動的に再開します。

5.16.2 AWI Tera1 クライアント : 電源承認

Power ページでは、クライアントのホスト電源オフ承認を設定することができます。このページは、**Permissions > Power** メニューからアクセスすることができます。



図 5-68 : AWI Tera1 クライアント Power ページ

表 5-65 : AWI Tera1 クライアント Power ページパラメータ

パラメータ	説明
Client Power Button	<p>このプロパティによって、クライアントのリモート PC ボタンの機能が設定されます。</p> <p>ホストは、クライアントのリモート PC ボタンの押下が 4 秒未満で、ソフト電源オフが有効になっている場合に、ソフト電源オフを実行（つまり、スリープモードに移行）するように指示されます。</p> <p>ホストは、クライアントのリモート PC ボタンの押下が 4 秒以上で、</p>

パラメータ	説明
	<p>ハード電源オフが有効になっている場合に、ハード電源オフ（つまり、シャットダウン）を実行するように指示されます。</p> <p>以下のオプションの中から選択します。</p> <ul style="list-style-type: none"> • Power-off not permitted : ユーザはホストをシャットダウンしたり、ホストをスリープモードに移行したりすることができません。 • Soft Power-off only : ユーザはホストをスリープモードに移行することはできますが、ホストをシャットダウンすることはできません。 • Hard Power-off only : ユーザはホストをシャットダウンすることはできますが、ホストをスリープモードに移行することはできません。 • Soft and Hard Power-off : ユーザはホストをスリープモードに移行することも、ホストをシャットダウンすることもできます。

5.17 ホストドライバ機能の設定

5.17.1 MC : ホストドライバ機能

このページの設定を使用すれば、ホストコンピュータ上で PCoIP ホストソフトウェア UI を有効または無効にするようにプロファイルを設定することができます。

注意 : PCoIP ホストソフトウェアのインストール方法と使用方法については、『PCoIP Host Software User Guide』（TER0810001）を参照してください。

MC でプロパティを有効にするには、**Set in Profile** チェックボックスをオンにし、指示に従ってフィールドを設定します。このページでプロパティを更新したら、**Save** をクリックして変更を保存します。

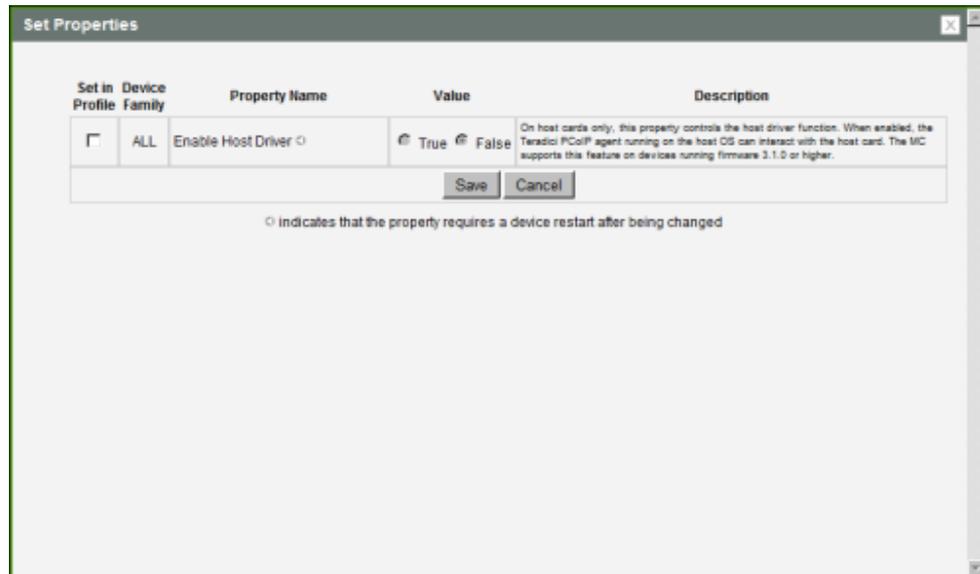


図 5-69 : MC ホストドライバ設定

表 5-66 : MC ホストドライバ設定パラメータ

パラメータ	説明
Enable Host Driver	<p>有効になっている場合は、ホストコンピュータ上の PCoIP ホストソフトウェアにアクセスすることができます。このソフトウェアを使用すれば、以下のような機能を有効にすることができます。</p> <ul style="list-style-type: none"> ローカルカーソルとキーボード機能の使用 セッションが中断したときのホスト PC のロック Wake-on-LAN 機能の使用 ホストとクライアントのネットワークパラメータの表示 セッションの切断 ホストの統計情報と接続情報の表示 ホスト上でのクライアントディスプレイトポロジ設定の使用 <p>無効になっている場合は、ホストコンピュータ上の PCoIP ホストソフトウェア UI にアクセスすることができません。</p> <p style="color: green;">注意：このプロパティを変更した場合はデバイスを再起動する必要があります。</p>

5.17.2 AWI ホスト : ホストドライバ機能

このページの設定を使用すれば、ホストコンピュータ上で PCoIP ホストソフトウェア UI を有効または無効にすることができます。このページは、**Configuration > Host Driver Function** メニューからアクセスすることができます。

注意：PCoIP ホストソフトウェアのインストール方法と使用方法については、『PCoIP Host Software User Guide』（TER0810001）を参照してください。



図 5-70 : AWI Host Driver Function ページ

表 5-67 : AWI ホストドライバ機能パラメータ

パラメータ	説明
Enable Host Driver Function	<p>有効になっている場合は、ホストコンピュータ上の PCoIP ホストソフトウェアにアクセスすることができます。このソフトウェアを使用すれば、以下のような機能を有効にすることができます。</p> <ul style="list-style-type: none"> ローカルカーソルとキーボード機能の使用 セッションが中断したときのホスト PC のロック Wake-on-LAN 機能の使用 ホストとクライアントのネットワークパラメータの表示 セッションの切断 ホストの統計情報と接続情報の表示 ホスト上でのクライアントディスプレイポロジ設定の使用 <p>無効になっている場合は、ホストコンピュータ上の PCoIP ホストソフトウェア UI にアクセスすることができません。</p>

5.18 イベントログの設定

5.18.1 MC : イベントログ設定

このページの設定を使用すれば、ホストやクライアントに使用したり、デバイス上のログフィルタリングモードを設定したりするためのイベントログメッセージングでプロファイルを構成することができます。

syslog を有効にして、イベントを収集して報告するためのロギングプロトコルとして設定することもできます。

MC でプロパティを有効にするには、**Set in Profile** チェックボックスをオンにし、指示に従ってフィールドを設定します。このページでプロパティを更新したら、**Save** をクリックして変更を保存します。

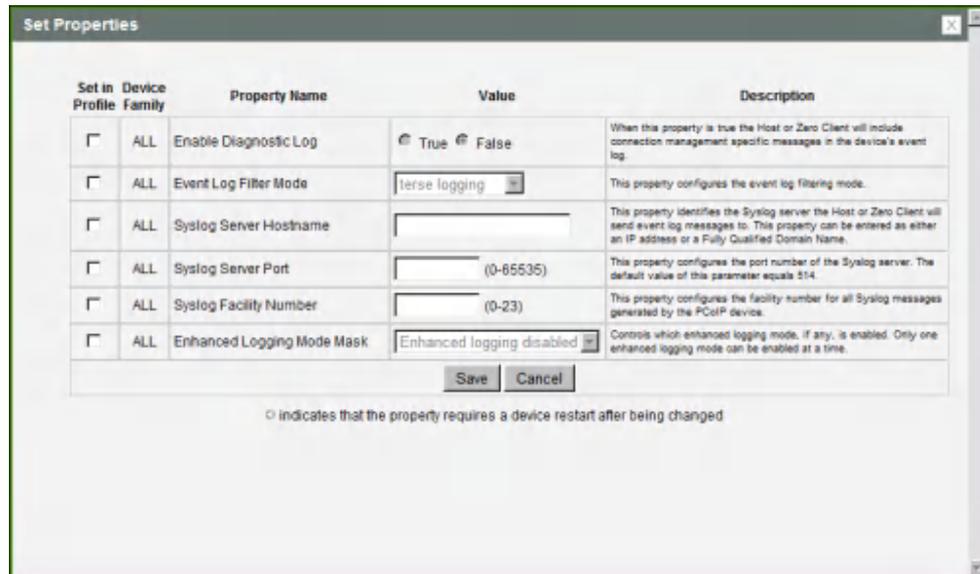


図 5-71 : MC イベントログ管理

表 5-68 : MC イベントログ管理パラメータ

パラメータ	説明
Enable Diagnostic Log	有効になっている場合は、デバイスのイベントログに接続管理固有のメッセージが追加されます。
Event Log Filter Mode	イベントログフィルタリングモードを簡潔または冗長として設定します。
Syslog Server Hostname	ホストまたはクライアントがイベントログメッセージを送信する syslog サーバの IP アドレスまたは完全修飾ドメイン名を入力します。
Syslog Server Port	syslog サーバのポート番号を入力します。 注意：ポート番号のデフォルト値は 514 です。
Syslog Facility Number	デバイスで生成されるすべての syslog メッセージのファシリティ番号を入力します。
Enhanced Logging Mode Mask	拡張ロギングモードを有効にするには、以下のカテゴリのいずれかを選択します。 <ul style="list-style-type: none"> • Audio • Management Console • Video • Networking • Session Negotiation • Smart Card

パラメータ	説明
	<ul style="list-style-type: none"> • System • USB • OneSign <p style="color: green;">注意：一度に有効にできるのは、上記カテゴリのいずれか1つの拡張ロギングだけです。</p>

5.18.2 AWI：イベントログ設定

Event Log ページでは、ホストまたはクライアントからのイベントログメッセージを表示または消去したり、デバイス上のログフィルタリングモードを設定したりすることができます。このページは、ホストまたはクライアントの **Diagnostics > Event Log** メニューからアクセスすることができます。

syslog を有効にして、イベントを収集して報告するためのロギングプロトコルとして設定することもできます。

Event Log
Configure diagnostic logging options

Event Log Messages:

Event Log Filter Mode:

Enable Syslog:

Identify Syslog Host By: IP address FQDN

Syslog Host IP Address: . . .

Syslog Host Port:

Syslog Facility:

Enhanced logging mode:

Category	Enable enhanced logging
AUDIO	<input type="radio"/>
MANAGEMENT CONSOLE	<input type="radio"/>
NETWORKING	<input type="radio"/>
ONESIGN	<input type="radio"/>
SESSION NEGOTIATION	<input type="radio"/>
SMARTCARD	<input type="radio"/>
SYSTEM	<input type="radio"/>
USB	<input type="radio"/>

図 5-72 : AWI Event Log ページ

表 5-69 : AWI Event Log ページパラメータ

パラメータ	説明
Event log Messages	<p>View : クリックすると、ブラウザページが開いて、デバイス上に保存されたイベントログメッセージ（タイムスタンプ情報付き）が表示されます。ブラウザページのログ情報を更新するには、F5を押します。</p> <p>Clear : クリックすると、デバイス上に保存されたすべてのイベントログメッセージが削除されます。</p>
Event Log Filter Mode	<p>プルダウンメニューをクリックしてイベントログフィルタリングモードを選択します。</p> <ul style="list-style-type: none"> • Verbose (デフォルト設定) • Terse

パラメータ	説明
Enable Syslog	<p>syslog 標準をデバイスのロギングメカニズムとして有効または無効にします。</p> <p>注意：syslog が有効になっている場合は、残りのフィールドを設定する必要があります。syslog が無効になっている場合は、これらのフィールドを編集することができません。</p>
Identify Syslog Host By	<p>syslog サーバホストを IP アドレスで識別するか、完全修飾ドメイン名 (FQDN) で識別するかを選択します。</p>
Syslog Host IP Address / Syslog Host DNS name	<p>表示されるパラメータは、syslog サーバホストを識別するために選択したオプションによって異なります。</p> <ul style="list-style-type: none"> • IP Address : syslog サーバホストの IP アドレスを入力します。 • FQDN : syslog サーバホストの DNS 名を入力します。 <p>注意：無効な IP アドレスまたは DNS 名を入力した場合は、その修正を促すメッセージが表示されます。</p>
Syslog Host Port	<p>syslog サーバのポート番号を入力します。</p> <p>注意：ポート番号のデフォルト値は 514 です。</p>
Syslog Facility	<p>ファシリティは、syslog メッセージのソースを分類するためにすべての syslog メッセージに付加される番号です。このファシリティは、標準 syslog ヘッダの一部であり、すべての syslog サーバで解釈されます。</p> <p>ロギングニーズに適したファシリティを入力します。例えば、次のようにデバイスを設定することができます。</p> <ul style="list-style-type: none"> • ゼロクライアントがファシリティ 19 を使用する • Cisco ルータがファシリティ 20 を使用する • VMware ESX ホストがファシリティ 21 を使用する <p>注意：デフォルトファシリティは「19 – local use 3」に設定されません。Cisco ルータはデフォルトで「23 – local use 7」に設定されません。</p>
Enhanced logging mode	<p>拡張ロギングモードを有効にするには、以下のカテゴリのいずれかを選択します。</p> <ul style="list-style-type: none"> • Audio • Management Console • Video • Networking • Session Negotiation • Smart Card • System • USB

パラメータ	説明
	<ul style="list-style-type: none"> OneSign 注意：一度に有効にできるのは、上記カテゴリのいずれか1つの拡張ロギングだけです。

5.18.3 OSD : イベントログ設定

Event Log ページでは、クライアントからのイベントログメッセージを表示、更新、および消去することができます。このページは、**Options > Diagnostics > Event Log** メニューからアクセスすることができます。

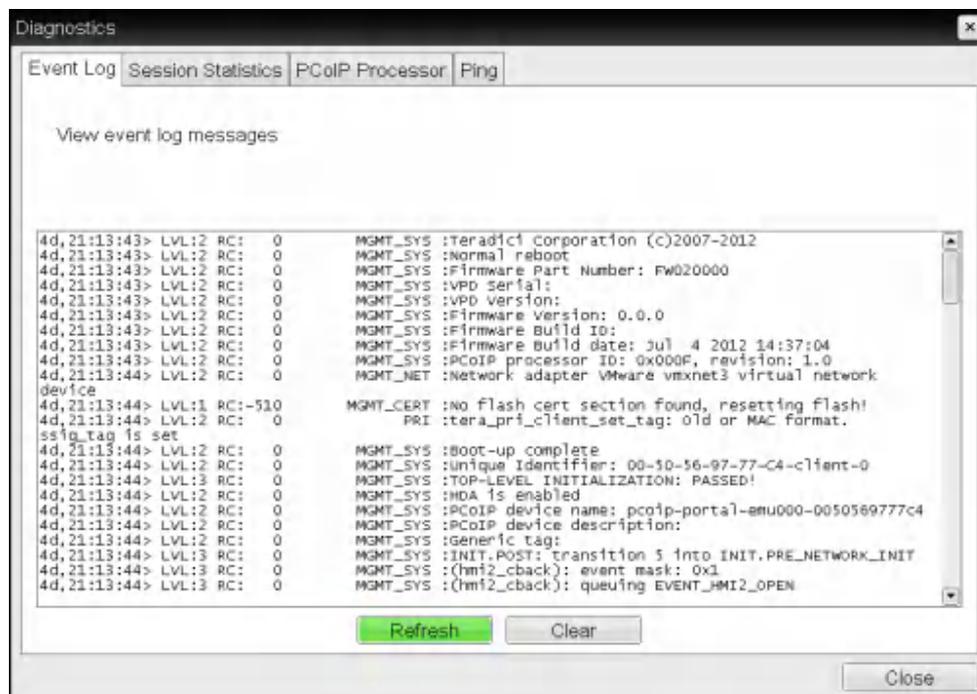


図 5-73 : OSD Event Log ページ

表 5-70 : OSD Event Log ページパラメータ

パラメータ	説明
Refresh	クリックすると、このページに表示されたログ情報が更新されます。
Clear	クリックすると、デバイス上に保存されたすべてのイベントログメッセージが削除されます。

5.19 周辺機器の設定

5.19.1 MC : 周辺機器設定

このページの設定を使用すれば、選択したデバイス上の USB Enhanced Host Controller Interface (EHCI) モードを有効または無効にするようにプロファイルを構成することができます。

MC でプロパティを有効にするには、**Set in Profile** チェックボックスをオンにし、指示に従ってフィールドを設定します。このページでプロパティを更新したら、**Save** をクリックして変更を保存します。

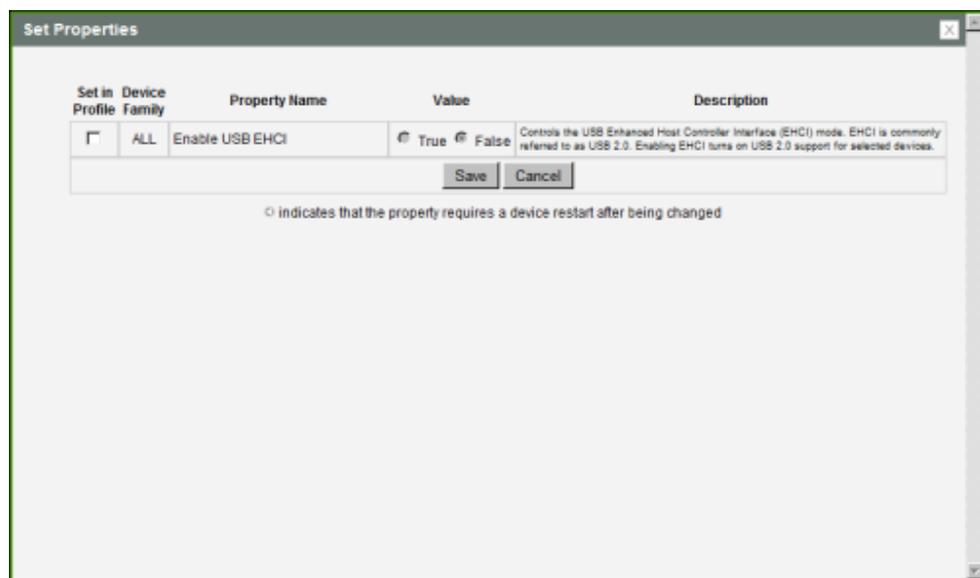


図 5-74 : MC 周辺機器設定

表 5-71 : MC 周辺機器設定パラメータ

パラメータ	説明
Enable USB EHCI	有効になっている場合は、VMware View 4.6 以降を実行しているホストとのセッション用のゼロクライアント USB ポートに直接接続されたデバイスの EHCI (USB 2.0) が設定されます。 注意 : RAM が 128MB 未満のクライアント上では、この機能を有効にすることができません。等時性エンドポイントを備えたデバイスは USB 2.0 の速度で動作しません。

5.19.2 AWI クライアント : 周辺機器設定に関するヘルプ

AWI の周辺機器 USB EHCI 設定は、[AWI Client : USB Permissions](#) ページ (**Permissions > USB** メニューからアクセス) に配置されています。

5.20 IPv6 の設定

5.20.1 MC : IPv6 設定

このページの設定を使用すれば、IPv6 ネットワークに接続された PCoIP デバイスの IPv6 を有効にするようにプロファイルを構成することができます。

注意：現時点で、VMware View は IPv6 に対応していません。

MC でプロパティを有効にするには、**Set in Profile** チェックボックスをオンにし、指示に従ってフィールドを設定します。このページでプロパティを更新したら、**Save** をクリックして変更を保存します。

Set in Profile	Device Family	Property Name	Value	Description
<input type="checkbox"/>	ALL	Enable IPv6	<input checked="" type="radio"/> True <input type="radio"/> False	This property determines if the endpoint uses IPv6. IPv6 is not enabled by default.
<input type="checkbox"/>	ALL	IPv6 Domain Name	<input type="text"/>	This property configures the IPv6 domain name. If DHCPv6 is enabled, this is the value returned by DHCPv6 otherwise it is the static setting.
<input type="checkbox"/>	ALL	Enable DHCPv6	<input checked="" type="radio"/> True <input type="radio"/> False	This property determines if the endpoint uses DHCPv6 to obtain IPv6 addresses (stored in IPv6 DHCP Address 1-4). DHCPv6 is enabled by default.
<input type="checkbox"/>	ALL	Enable SLAAC	<input checked="" type="radio"/> True <input type="radio"/> False	This property determines if the endpoint uses SLAAC (IPv6) to obtain IPv6 addresses (stored in IPv6 SLAAC Address 1-4). SLAAC is enabled by default.
<input type="checkbox"/>	ALL	IPv6 Gateway Address	<input type="text"/>	This property configures the IPv6 gateway address (e.g. "FD0F:EC91:10F9:201:215:50FF:FEA0:1585"). This is the value provided in Router Advertisements (if enabled), otherwise is the static setting.
<input type="checkbox"/>	ALL	IPv6 Gateway Address Prefix Length	<input type="text"/> (0-64)	This property configures the IPv6 gateway address prefix length (e.g. 64). This is the value provided in Router Advertisements (if enabled), otherwise is the static setting.
<input type="checkbox"/>	ALL	IPv6 Primary DNS Address	<input type="text"/>	This property configures the IPv6 address of the primary DNS server (e.g. "FD0F:EC91:10F9:201:215:50FF:FEA0:7624"). If DHCPv6 is enabled, this is the value returned by DHCPv6 otherwise it is the static setting.
<input type="checkbox"/>	ALL	IPv6 Primary DNS Address Prefix Length	<input type="text"/> (0-64)	This property configures the IPv6 address prefix length of the primary DNS server (e.g. 64). If DHCPv6 is enabled, this is the value returned by DHCPv6 otherwise it is the static setting.
<input type="checkbox"/>	ALL	IPv6 Secondary DNS Address	<input type="text"/>	This property configures the IPv6 address of the secondary DNS server (e.g. "FD0F:EC91:10F9:201:215:50FF:FEA0:7627"). If DHCPv6 is enabled, this is the value returned by DHCPv6 otherwise it is the static setting.
<input type="checkbox"/>	ALL	IPv6 Secondary DNS Address Prefix Length	<input type="text"/> (0-64)	This property configures the IPv6 address prefix length of the secondary DNS server (e.g. 64). If DHCPv6 is enabled, this is the value returned by DHCPv6 otherwise it is the static setting.

図 5-75 : MC IPv6 設定

表 5-72 : MC IPv6 設定パラメータ

パラメータ	説明
Enable IPv6	このプロパティは、デバイスが IPv6 を使用するかどうかを決定します。IPv6 はデフォルトで無効になっています。 注意：このプロパティを変更した場合はデバイスを再起動する必要があります。
IPv6 Domain Name	DHCPv6 が有効になっている場合は、これが DHCPv6 から返される値です。そうでない場合は、これが静的な設定になります。 注意：このプロパティを変更した場合はデバイスを再起動する必要があります。
Enable DHCPv6	デバイスが DHCPv6 を使用して IPv6 アドレス (IPv6 DHCP アドレス 1~4 に保存) を取得するかどうかを決定します。DHCPv6 はデフォ

パラメータ	説明
	<p>ルトで有効になっています。</p> <p>注意：このプロパティを変更した場合はデバイスを再起動する必要があります。</p>
Enable SLAAC	<p>エンドポイントがステータスアドレス自動設定（SLAAC IPv6）を使用して IPv6 アドレス（IPv6 SLAAC アドレス 1~4 に保存）を取得するかどうかを決定します。SLAAC はデフォルトで有効になっています。</p> <p>注意：このプロパティを変更した場合はデバイスを再起動する必要があります。</p>
IPv6 Gateway Address	<p>IPv6 ゲートウェイアドレスを設定します（"FD0F:EC91:16F9:201:215:58FF:FEA0:1565"など）。これは、ルータアダプタサイズメント（有効になっている場合）で指定された値です。有効になっていない場合は、これが静的な設定になります。</p> <p>注意：このプロパティを変更した場合はデバイスを再起動する必要があります。</p>
IPv6 Gateway Address Prefix Length	<p>IPv6 ゲートウェイアドレスプレフィックス長を設定します（64 など）。これは、ルータアダプタサイズメント（有効になっている場合）で指定された値です。有効になっていない場合は、これが静的な設定になります。</p> <p>注意：このプロパティを変更した場合はデバイスを再起動する必要があります。</p>
IPv6 Primary DNS Address	<p>プライマリ DNS サーバの IPv6 アドレスを設定します（"FD0F:EC91:16F9:201:215:58FF:FEA0:7824"など）。DHCPv6 が有効になっている場合は、これが DHCPv6 から返される値です。そうでない場合は、これが静的な設定になります。</p> <p>注意：このプロパティを変更した場合はデバイスを再起動する必要があります。</p>
IPv6 Primary DNS Address Prefix Length	<p>プライマリ DNS サーバの IPv6 アドレスプレフィックス長を設定します（64 など）。DHCPv6 が有効になっている場合は、これが DHCPv6 から返される値です。そうでない場合は、これが静的な設定になります。</p> <p>注意：このプロパティを変更した場合はデバイスを再起動する必要があります。</p>
IPv6 Secondary DNS Address	<p>セカンダリ DNS サーバの IPv6 アドレスを設定します（"FD0F:EC91:16F9:201:215:58FF:FEA0:7827"など）。DHCPv6 が有効になっている場合は、これが DHCPv6 から返される値です。そうでない場合は、これが静的な設定になります。</p> <p>注意：このプロパティを変更した場合はデバイスを再起動する必要があります。</p>

パラメータ	説明
	あります。
IPv6 Secondary DNS Address Prefix Length	セカンダリ DNS サーバの IPv6 アドレスプレフィックス長を設定します (64 など)。DHCPv6 が有効になっている場合は、これが DHCPv6 から返される値です。そうでない場合は、これが静的な設定になります。 注意：このプロパティを変更した場合はデバイスを再起動する必要があります。

5.20.2 AWI : IPv6 設定

このページの設定を使用すれば、IPv6 ネットワークに接続された PCoIP デバイスの IPv6 を有効にすることができます。

注意：現時点で、VMware View は IPv6 に対応していません。

このページは、ホストまたはクライアントの **Configuration > IPv6** メニューからアクセスすることができます。

IPv6

Change the IPv6 network settings for the device

Enable IPv6:

Link Local Address:

Gateway:

Enable DHCPv6:

Primary DNS:

Secondary DNS:

Domain Name:

FQDN:

Enable SLAAC:

Enable Manual Address:

図 5-76 : AWI IPv6 ページ

注意：このページ上でいずれかの設定を変更した場合は、変更を反映させるためにデバイスを再起動する必要があります。

表 5-73 : AWI IPv6 ページパラメータ

パラメータ	説明
Enable IPv6	このフィールドは、PCoIP デバイスの IPv6 を有効にする場合に有効にします。
Link Local Address	このフィールドは自動的に値が設定されます。
Gateway	IPv6 ゲートウェイアドレスを入力します。
Enable DHCPv6	このフィールドは、デバイスの動的ホスト構成プロトコルバージョン 6 (DHCPv6) をセットアップする場合に有効にします。
DHCPv6 Addresses	DHCPv6 が有効になっている状態でデバイスを再起動すると、サーバが自動的にこれらのフィールドをデバイスのアドレスに設定します。
Primary DNS	デバイスのプライマリ DNS IP アドレス。DHCPv6 が有効になっている場合は、DHCPv6 サーバによって自動的にこのフィールドに値が設定されます。
Secondary DNS	デバイスのセカンダリ DNS IP アドレス。DHCPv6 が有効になっている場合は、DHCPv6 サーバによって自動的にこのフィールドに値が設定されます。
Domain Name	ホストまたはクライアントで使用されるドメイン名 ("domain.local" など)。DHCPv6 が有効になっている場合は、DHCPv6 サーバによって自動的にこのフィールドに値が設定されます。
FQDN	ホストまたはクライアントの完全修飾ドメイン名。DHCPv6 が有効になっている場合は、DHCPv6 サーバによって自動的にこのフィールドに値が設定されます。
Enable SLAAC	このフィールドは、デバイスのステートレスアドレス自動設定 (SLAAC) をセットアップする場合に有効にします。
SLAAC Addresses	SLAAC が有効になっている状態でデバイスを再起動すると、これらのフィールドに自動的に値が設定されます。
Enable Manual Address	このフィールドは、デバイスの手動 (静的) アドレスをセットアップする場合に有効にします。
Manual Address	デバイスの IP アドレスを入力します。

5.20.3 OSD : IPv6 設定

このページの設定を使用すれば、IPv6 ネットワークに接続された PCoIP デバイスの IPv6 を有効にすることができます。

注意：現時点で、VMware View は IPv6 に対応していません。

このページは、**Options > Configuration > IPv6** メニューからアクセスすることができます。

The screenshot shows a 'Configuration' dialog box with the 'IPv6' tab selected. The dialog contains the following settings:

- Enable IPv6:
- Link Local Address:
- Gateway:
- Enable DHCPv6: /64
- Primary DNS:
- Secondary DNS:
- Domain Name:
- FQDN:
- Enable SLAAC: /64
- Enable Manual Address:
- Manual Address:

Buttons at the bottom: Unlock, OK (highlighted in green), Cancel, Apply.

図 5-77 : OSD IPv6 ページ

注意：このページ上でいずれかの設定を変更した場合は、変更を反映させるためにデバイスを再起動する必要があります。

表 5-74 : OSD IPv6 ページパラメータ

パラメータ	説明
Enable IPv6	このフィールドは、PCoIP デバイスの IPv6 を有効にする場合に有効にします。
Link Local Address	このフィールドは自動的に値が設定されます。
Gateway	IPv6 ゲートウェイアドレスを入力します。

パラメータ	説明
Enable DHCPv6	このフィールドは、デバイスの動的ホスト構成プロトコルバージョン 6 (DHCPv6) をセットアップする場合に有効にします。
DHCPv6 Addresses	DHCPv6 が有効になっている状態でデバイスを再起動すると、サーバが自動的にこれらのフィールドをデバイスのアドレスに設定します。
Primary DNS	デバイスのプライマリ DNS IP アドレス。DHCPv6 が有効になっている場合は、DHCPv6 サーバによって自動的にこのフィールドに値が設定されます。
Secondary DNS	デバイスのセカンダリ DNS IP アドレス。DHCPv6 が有効になっている場合は、DHCPv6 サーバによって自動的にこのフィールドに値が設定されます。
Domain Name	ホストまたはクライアントで使用されるドメイン名 ("domain.local" など)。DHCPv6 が有効になっている場合は、DHCPv6 サーバによって自動的にこのフィールドに値が設定されます。
FQDN	ホストまたはクライアントの完全修飾ドメイン名。DHCPv6 が有効になっている場合は、DHCPv6 サーバによって自動的にこのフィールドに値が設定されます。
Enable SLAAC	このフィールドは、デバイスのステータスアドレス自動設定 (SLAAC) をセットアップする場合に有効にします。
SLAAC Addresses	SLAAC が有効になっている状態でデバイスを再起動すると、これらのフィールドに自動的に値が設定されます。
Enable Manual Address	このフィールドは、デバイスの手動 (静的) アドレスをセットアップする場合に有効にします。
Manual Address	デバイスの IP アドレスを入力します。

5.21 ディスプレイトポロジの設定

5.21.1 MC : ディスプレイトポロジ設定

このページの設定を使用すれば、Tera1 クライアントと Tera2 クライアントに使用されるディスプレイトポロジでプロファイルを構成することができます。

注意 : TERA2321 ゼロクライアントデバイスの場合、デュアルディスプレイゼロクライアントレイアウトを使用してください。

MC でプロパティを有効にするには、**Set in Profile** チェックボックスをオンにし、指示に従ってフィールドを設定します。このページでプロパティを更新したら、**Save** をクリックして変更を保存します。

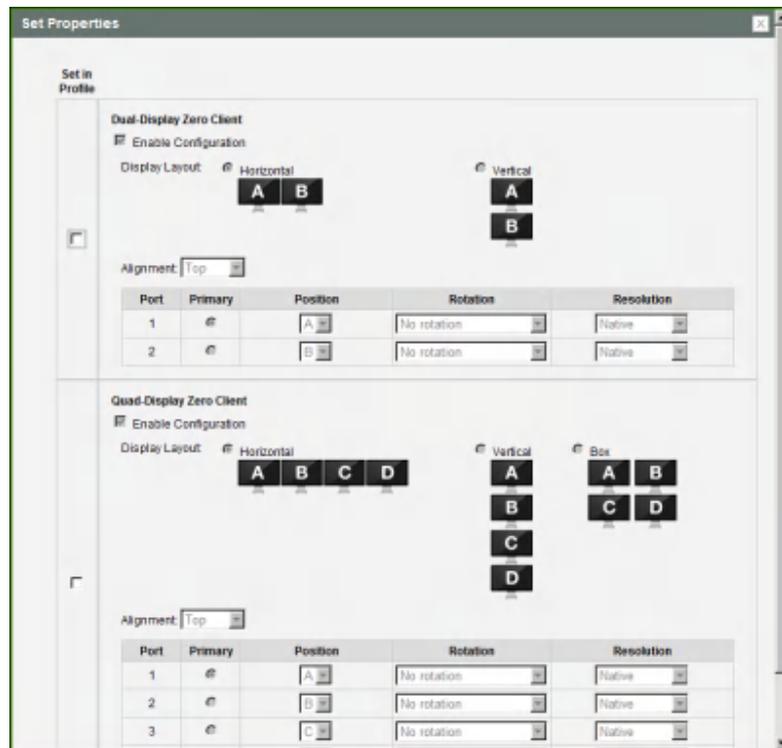


図 5-78 : MC ディスプレイポートロジ設定

表 5-75 : MC ディスプレイポートロジ設定パラメータ

パラメータ	説明
デュアルディスプレイゼロクライアント	
Enable Configuration	PCoIP チップセットあたり 2 台のディスプレイをサポートするようにデバイスを設定する場合に有効にします。
Display Layout	ディスプレイのレイアウトを選択します (A と B)。この設定は、机上のディスプレイの物理的なレイアウトを反映している必要があります。 <ul style="list-style-type: none"> • Horizontal : 図に示すように、ディスプレイを横方向に配置する場合に選択します。 • Vertical : 図に示すように、ディスプレイを縦方向に配置する場合に選択します。
Alignment	ディスプレイのサイズが異なる場合の配置方法を選択します。 注意 : この設定は、ユーザがディスプレイ間でカーソルを移動すると

パラメータ	説明
	<p>きに使用される画面の領域に影響を与えます。ドロップダウンリストに表示される整列オプションは、選択されたディスプレイレイアウトによって異なります。</p> <p>Horizontal layout :</p> <ul style="list-style-type: none"> • Top : ディスプレイを上側で揃える場合に選択します。この設定では、サイズが異なるディスプレイ間のナビゲート時に画面の上部領域が使用されます。 • Center : ディスプレイを横方向の中央に配置する場合に選択します。この設定では、サイズが異なるディスプレイ間のナビゲート時に画面の中央領域が使用されます。 • Bottom : ディスプレイを下側で揃える場合に選択します。この設定では、サイズが異なるディスプレイ間のナビゲート時に画面の下部領域が使用されます。 <p>Vertical layout :</p> <ul style="list-style-type: none"> • Left : ディスプレイを左側で揃える場合に選択します。この設定では、サイズが異なるディスプレイ間のナビゲート時に画面の左領域が使用されます。 • Center : ディスプレイを縦方向の中央に配置する場合に選択します。この設定では、サイズが異なるディスプレイ間のナビゲート時に画面の中央領域が使用されます。 • Right : ディスプレイを右側で揃える場合に選択します。この設定では、サイズが異なるディスプレイ間のナビゲート時に画面の右領域が使用されます。
Primary	<p>プライマリポートにするゼロクライアント上のビデオポートを設定します。</p> <p>注意 : プライマリポートに接続されたディスプレイがプライマリディスプレイ (つまり、PCoIP セッションを開始する前に OSD メニューが表示され、セッションの開始後に Windows のタスクバーが要求されるディスプレイ) になります。</p> <ul style="list-style-type: none"> • Port 1 : ゼロクライアント上のポート 1 をプライマリポートとして設定する場合に選択します。 • Port 2 : ゼロクライアント上のポート 2 をプライマリポートとして設定する場合に選択します。
Position	各ポートに物理的に接続するディスプレイを指定します。
Rotation	<p>各ポートのディスプレイの回転を設定します。</p> <ul style="list-style-type: none"> • No rotation • 90° clockwise • 180° rotation • 90° counter-clockwise
Resolution	ディスプレイ解像度は、仮想マシンまたはホストとゼロクライアント間の PCoIP セッション用に設定することができます。ゼロクライアント

パラメータ	説明
	<p>ントは、サポートされているモニタのディスプレイ解像度を検出して、それらをドロップダウンメニューに設定します。デフォルトでは、ディスプレイのネイティブ解像度が使用されます。</p>
クアッドディスプレイゼロクライアント	
Enable Configuration	PCoIP チップセットあたり 4 台のディスプレイをサポートするようにデバイスを設定する場合に有効にします。
Display Layout	<p>ディスプレイのレイアウトを選択します (A、B、C、および D)。この設定は、机上のディスプレイの物理的なレイアウトを反映している必要があります。</p> <ul style="list-style-type: none"> • Horizontal : 図に示すように、ディスプレイを横方向に配置する場合に選択します。 • Vertical : 図に示すように、ディスプレイを縦方向に配置する場合に選択します。 • Box : 図に示すように、ディスプレイをボックス構成で配置する場合に選択します。
Alignment	<p>ディスプレイのサイズが異なる場合の配置方法を選択します。</p> <p>注意：この設定は、ユーザがディスプレイ間でカーソルを移動するときに使用される画面の領域に影響を与えます。ドロップダウンリストに表示される整列オプションは、選択されたディスプレイレイアウトによって異なります。</p> <p>Horizontal layout :</p> <ul style="list-style-type: none"> • Top : ディスプレイを上側で揃える場合に選択します。この設定では、サイズが異なるディスプレイ間のナビゲート時に画面の上部領域が使用されます。 • Center : ディスプレイを横方向の中央に配置する場合に選択します。この設定では、サイズが異なるディスプレイ間のナビゲート時に画面の中央領域が使用されます。 • Bottom : ディスプレイを下側で揃える場合に選択します。この設定では、サイズが異なるディスプレイ間のナビゲート時に画面の下部領域が使用されます。 <p>Vertical layout :</p> <ul style="list-style-type: none"> • Left : ディスプレイを左側で揃える場合に選択します。この設定では、サイズが異なるディスプレイ間のナビゲート時に画面の左領域が使用されます。 • Center : ディスプレイを縦方向の中央に配置する場合に選択します。この設定では、サイズが異なるディスプレイ間のナビゲート時に画面の中央領域が使用されます。 • Right : ディスプレイを右側で揃える場合に選択します。この設定では、サイズが異なるディスプレイ間のナビゲート時に画面の右領域が使用されます。

パラメータ	説明
Primary	<p>プライマリポートにするゼロクライアント上のビデオポートを設定します。</p> <p>注意：プライマリポートに接続されたディスプレイがプライマリディスプレイ（つまり、PCoIP セッションを開始する前に OSD メニューが表示され、セッションの開始後に Windows のタスクバーが要求されるディスプレイ）になります。</p> <ul style="list-style-type: none"> • Port 1：ゼロクライアント上のポート 1 をプライマリポートとして設定する場合に選択します。 • Port 2：ゼロクライアント上のポート 2 をプライマリポートとして設定する場合に選択します。 • Port 3：ゼロクライアント上のポート 3 をプライマリポートとして設定する場合に選択します。 • Port 4：ゼロクライアント上のポート 4 をプライマリポートとして設定する場合に選択します。
Position	各ポートに物理的に接続するディスプレイを指定します。
Rotation	<p>各ポートのディスプレイの回転を設定します。</p> <ul style="list-style-type: none"> • No rotation • 90° clockwise • 180° rotation • 90° counter-clockwise
Resolution	<p>ディスプレイ解像度は、仮想マシンまたはホストとゼロクライアント間の PCoIP セッション用に設定することができます。ゼロクライアントは、サポートされているモニタのディスプレイ解像度を検出して、それらをドロップダウンメニューに設定します。デフォルトでは、ディスプレイのネイティブ解像度が使用されます。</p>

5.21.2 OSD デュアルディスプレイ：ディスプレイトポロジ設定

Display Topology ページでは、PCoIP セッション用のディスプレイトポロジを変更することができます。このページは、クライアント OSD の **Options > User Settings > Display Topology** メニューからアクセスすることができます。

クライアントと VMware View 仮想デスクトップ間の PCoIP セッションにディスプレイトポロジ機能を適用するには、VMware View 4.5 以降を使用する必要があります。クライアントと PCoIP ホスト間の PCoIP セッションにディスプレイトポロジ機能を適用するには、PCoIP ホストソフトウェアをホストにインストールしておく必要があります。

注意：ディスプレイトポロジ設定は、必ず、この **OSD Display Topology** ページを使用して変更してください。VMware View を使用している場合は、仮想マシン内の Windows ディスプレイ設定を使用し、これらの設定を変更しないようにしてください。

注意：クライアントとして TERA2321 ゼロクライアントデバイスを使用している場合は、このページにデュアルモニタレイアウトも表示されます。

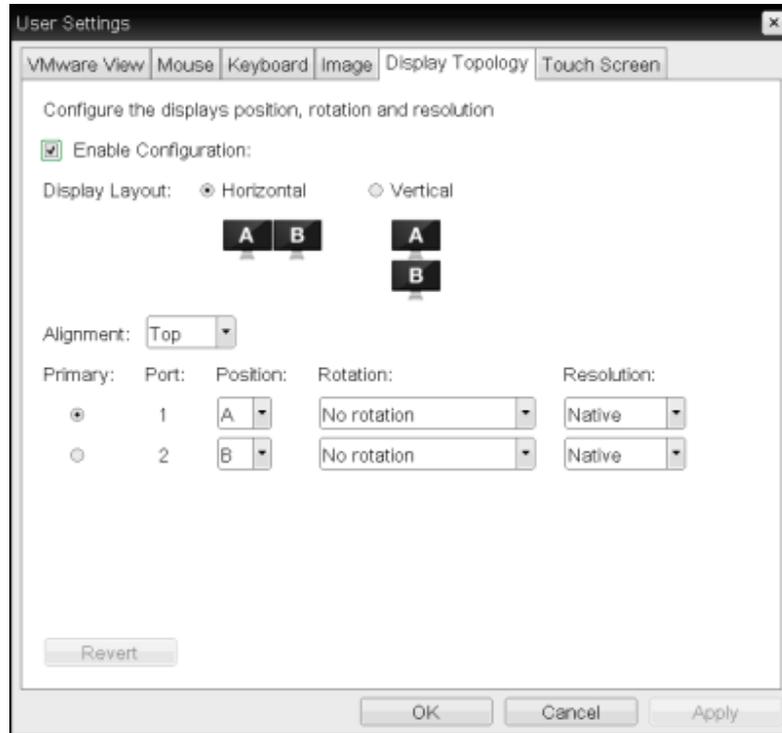


図 5-79 : OSD Tera1 Display Topology ページ

表 5-76 : OSD Tera1 Display Topology ページパラメータ

パラメータ	説明
Enable Configuration	PCoIP チップセットあたり 2 台のディスプレイをサポートするようにデバイスを設定する場合に有効にします。
Display Layout	<p>ディスプレイのレイアウトを選択します (A と B)。この設定は、机上のディスプレイの物理的なレイアウトを反映している必要があります。</p> <ul style="list-style-type: none"> • Horizontal : 図に示すように、ディスプレイを横方向に配置する場合に選択します。 • Vertical : 図に示すように、ディスプレイを縦方向に配置する場合に選択します。
Alignment	<p>ディスプレイのサイズが異なる場合の配置方法を選択します。</p> <p>注意：この設定は、ユーザがディスプレイ間でカーソルを移動するときに使用される画面の領域に影響を与えます。ドロップダウンリストに表示される整列オプションは、選択されたディスプレイレイアウトによって異なります。</p>

パラメータ	説明
	<p>Horizontal layout :</p> <ul style="list-style-type: none"> • Top : ディスプレイを上側で揃える場合に選択します。この設定では、サイズが異なるディスプレイ間のナビゲート時に画面の上部領域が使用されます。 • Center : ディスプレイを横方向の中央に配置する場合に選択します。この設定では、サイズが異なるディスプレイ間のナビゲート時に画面の中央領域が使用されます。 • Bottom : ディスプレイを下側で揃える場合に選択します。この設定では、サイズが異なるディスプレイ間のナビゲート時に画面の下部領域が使用されます。 <p>Vertical layout :</p> <ul style="list-style-type: none"> • Left : ディスプレイを左側で揃える場合に選択します。この設定では、サイズが異なるディスプレイ間のナビゲート時に画面の左領域が使用されます。 • Center : ディスプレイを縦方向の中央に配置する場合に選択します。この設定では、サイズが異なるディスプレイ間のナビゲート時に画面の中央領域が使用されます。 • Right : ディスプレイを右側で揃える場合に選択します。この設定では、サイズが異なるディスプレイ間のナビゲート時に画面の右領域が使用されます。
Primary	<p>プライマリポートにするゼロクライアント上のビデオポートを設定します。</p> <p>注意：プライマリポートに接続されたディスプレイがプライマリディスプレイ（つまり、PCoIPセッションを開始する前にOSDメニューが表示され、セッションの開始後にWindowsのタスクバーが要求されるディスプレイ）になります。</p> <ul style="list-style-type: none"> • Port 1 : ゼロクライアント上のポート1をプライマリポートとして設定する場合に選択します。 • Port 2 : ゼロクライアント上のポート2をプライマリポートとして設定する場合に選択します。
Position	各ポートに物理的に接続するディスプレイを指定します。
Rotation	<p>各ポートのディスプレイの回転を設定します。</p> <ul style="list-style-type: none"> • No rotation • 90° clockwise • 180° rotation • 90° counter-clockwise
Resolution	<p>ディスプレイ解像度は、仮想マシンまたはホストとゼロクライアント間のPCoIPセッション用に設定することができます。ゼロクライアントは、サポートされているモニタのディスプレイ解像度を検出して、それらをドロップダウンメニューに設定します。デフォルトでは、ディスプレイのネイティブ解像度が使用されます。</p>

5.21.3 OSD クアッドディスプレイ : ディスプレイトポロジ設定

Display Topology ページでは、PCoIPセッション用のディスプレイトポロジを変更することができます。このページは、クライアント OSD の **Options > User Settings > Display Topology** メニューからアクセスすることができます。

クライアントと VMware View 仮想デスクトップ間の PCoIPセッションにディスプレイトポロジ機能を適用するには、VMware View 4.5 以降を使用する必要があります。クライアントと PCoIP ホスト間の PCoIPセッションにディスプレイトポロジ機能を適用するには、PCoIP ホストソフトウェアをホストにインストールしておく必要があります。

注意：ディスプレイトポロジ設定は、必ず、この **OSD Display Topology** ページを使用して変更してください。VMware View を使用している場合は、仮想マシン内の **Windows** ディスプレイ設定を使用し、これらの設定を変更しないようにしてください。

注意：クライアントとして TERA2321 ゼロクライアントデバイスを使用している場合は、このページに、クアッドモニタレイアウトの代わりに、[デュアルモニタレイアウト](#)が表示されます。

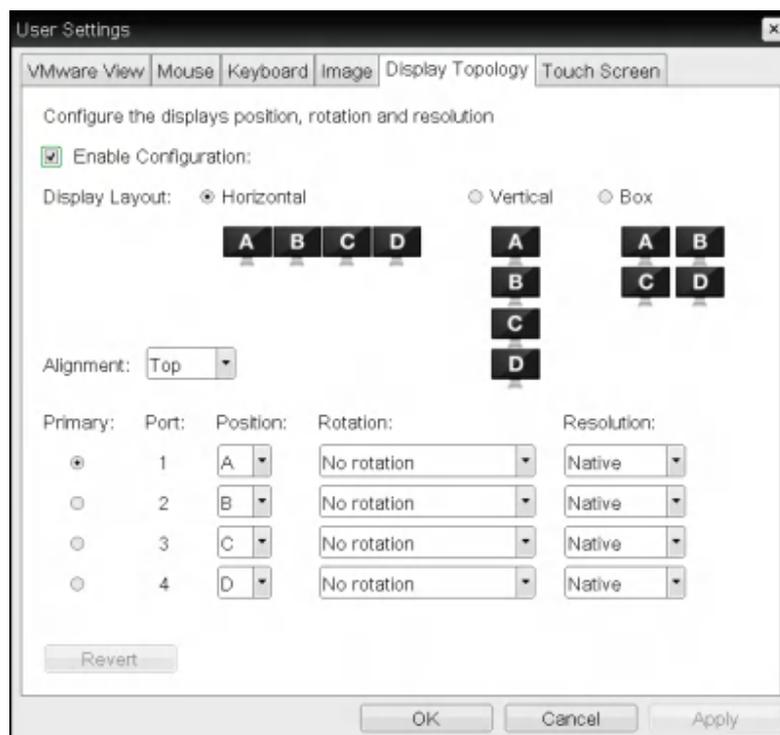


図 5-80 : OSD Tera2 Display Topology ページ

表 5-77 : OSD Tera2 Display Topology ページパラメータ

パラメータ	説明
-------	----

パラメータ	説明
Enable Configuration	PCoIP チップセットあたり 4 台のディスプレイをサポートするようにデバイスを設定する場合に有効にします。
Display Layout	<p>ディスプレイのレイアウトを選択します (A、B、C、および D)。この設定は、机上のディスプレイの物理的なレイアウトを反映している必要があります。</p> <ul style="list-style-type: none"> • Horizontal : 図に示すように、ディスプレイを横方向に配置する場合に選択します。 • Vertical : 図に示すように、ディスプレイを縦方向に配置する場合に選択します。 • Box : 図に示すように、ディスプレイをボックス構成で配置する場合に選択します。
Alignment	<p>ディスプレイのサイズが異なる場合の配置方法を選択します。</p> <p>注意：この設定は、ユーザがディスプレイ間でカーソルを移動するときに使用される画面の領域に影響を与えます。ドロップダウンリストに表示される整列オプションは、選択されたディスプレイレイアウトによって異なります。</p> <p>Horizontal layout :</p> <ul style="list-style-type: none"> • Top : ディスプレイを上側で揃える場合に選択します。この設定では、サイズが異なるディスプレイ間のナビゲート時に画面の上部領域が使用されます。 • Center : ディスプレイを横方向の中央に配置する場合に選択します。この設定では、サイズが異なるディスプレイ間のナビゲート時に画面の中央領域が使用されます。 • Bottom : ディスプレイを下側で揃える場合に選択します。この設定では、サイズが異なるディスプレイ間のナビゲート時に画面の下部領域が使用されます。 <p>Vertical layout :</p> <ul style="list-style-type: none"> • Left : ディスプレイを左側で揃える場合に選択します。この設定では、サイズが異なるディスプレイ間のナビゲート時に画面の左領域が使用されます。 • Center : ディスプレイを縦方向の中央に配置する場合に選択します。この設定では、サイズが異なるディスプレイ間のナビゲート時に画面の中央領域が使用されます。 • Right : ディスプレイを右側で揃える場合に選択します。この設定では、サイズが異なるディスプレイ間のナビゲート時に画面の右領域が使用されます。
Primary	<p>プライマリポートにするゼロクライアント上のビデオポートを設定します。</p> <p>注意：プライマリポートに接続されたディスプレイがプライマリディスプレイ (つまり、PCoIP セッションを開始する前に OSD メニューが表示され、セッションの開始後に Windows のタスクバーが要求されるディスプレイ) になります。</p>

パラメータ	説明
	<ul style="list-style-type: none"> • Port 1 : ゼロクライアント上のポート 1 をプライマリポートとして設定する場合に選択します。 • Port 2 : ゼロクライアント上のポート 2 をプライマリポートとして設定する場合に選択します。 • Port 3 : ゼロクライアント上のポート 3 をプライマリポートとして設定する場合に選択します。 • Port 4 : ゼロクライアント上のポート 4 をプライマリポートとして設定する場合に選択します。
Position	各ポートに物理的に接続するディスプレイを指定します。
Rotation	各ポートのディスプレイの回転を設定します。 <ul style="list-style-type: none"> • No rotation • 90° clockwise • 180° rotation • 90° counter-clockwise
Resolution	ディスプレイ解像度は、仮想マシンまたはホストとゼロクライアント間の PCoIP セッション用に設定することができます。ゼロクライアントは、サポートされているモニタのディスプレイ解像度を検出して、それらをドロップダウンメニューに設定します。デフォルトでは、ディスプレイのネイティブ解像度が使用されます。

5.22 OSD ロゴのアップロード

5.22.1 MC : OSD ログ設定

Profile OSD Logo セクションは、管理コンソールの **Manage Profiles** ページの下部に配置されています。このセクションでは、ユーザのローカルオンスクリーンディスプレイ (OSD) GUI の **Connect** ページに表示されるプロファイルにイメージをアップロードすることができます。

注意 : **AWI Session – View Connection Server** ページの詳細オプションで [Use OSD Logo for View Banner](#) を有効にすることにより、VMware View バナーの代わりにこのロゴを表示するように **VMware View** ログイン画面を設定することができます。



図 5-81 : MC Profile OSD Logo 設定

Set OSD Logo をクリックすると、イメージファイルをアップロード可能な以下の画面が表示されます。

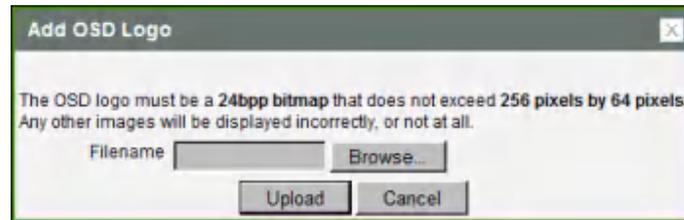


図 5-82 : MC Add OSD Logo 設定

表 5-78 : MC Add OSD Logo 設定パラメータ

パラメータ	説明
Filename	アップロードするロゴイメージのファイル名を指定します。 Browse ボタンを使用してターゲットファイルを参照することができます。 ファイルはウェブブラウザからアクセスできる必要があります（つまり、ローカルドライブまたはアクセス可能なネットワークドライブ上に存在する必要があります）。 24 bpp （ビット/ピクセル）イメージを BMP 形式にする必要があります、その寸法は幅が 256 ピクセル、高さが 64 ピクセルを超えないようにする必要があります。ファイル拡張子が間違っている場合はエラーメッセージが表示されます。
Upload	Upload をクリックすると指定されたイメージファイルがクライアントに転送されます。アップロードを確定するためのメッセージが表示されます。

5.22.2 AWI クライアント : OSD ロゴ設定

OSD Logo ページでは、ローカルオンスクリーンディスプレイ（OSD）GUI の **Connect** ページに表示するイメージをアップロードすることができます。**OSD Logo** ページは、**Upload > OSD Logo** メニューからアクセスすることができます。

注意 : **AWI Session – View Connection Server** ページの詳細オプションで **Use OSD Logo for View Banner** を有効にすることにより、VMware View バナーの代わりにこのロゴを表示するように **VMware View** ログイン画面を設定することができます。

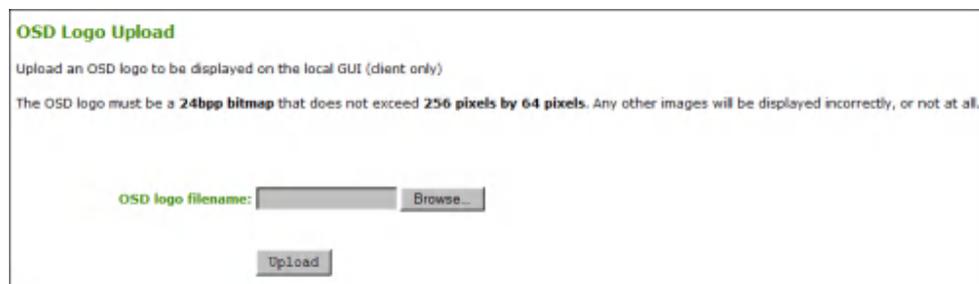


図 5-83 : AWI クライアント OSD Logo Upload ページ

表 5-79 : AWI クライアント OSD Logo Upload ページパラメータ

パラメータ	説明
OSD logo filename	アップロードするロゴイメージのファイル名を指定します。 Browse ボタンを使用してターゲットファイルを参照することができます。 ファイルはウェブブラウザからアクセスできる必要があります（つまり、ローカルドライブまたはアクセス可能なネットワークドライブ上に存在する必要があります）。 24 bpp （ビット/ピクセル）イメージを BMP 形式にする必要があります、その寸法は幅が 256 ピクセル、高さが 64 ピクセルを超えないようにする必要があります。ファイル拡張子が間違っている場合はエラーメッセージが表示されます。
Upload	Upload をクリックすると指定されたイメージファイルがクライアントに転送されます。アップロードを確認するためのメッセージが表示されます。

5.23 ファームウェアのアップロード

5.23.1 MC : ファームウェア管理

Profile Firmware セクションは、管理コンソールの **Manage Profiles** ページの下部に配置されています。このセクションでは、ファームウェアファイルをプロファイルに割り当て、ファームウェアが各デバイスに転送される前に満たすべきアップグレード基準を設定することができます。

注意：ファームウェアファイルをプロファイルに割り当てるためには、まず、**Update > Import Firmware** メニューを通してファイルが MC にインポートされていることを確認する必要があります。詳細については、『PCoIP Management Console User Manual』（TER0812002）を参照してください。



図 5-84 : MC Profile Firmware 設定

Set Firmware をクリックすると、次のような画面が表示されます。

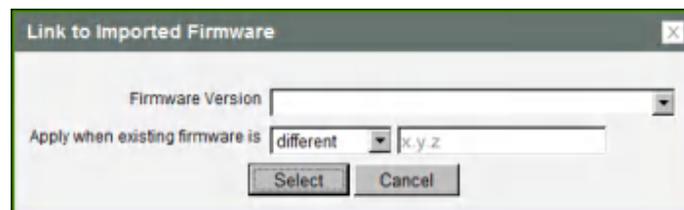


図 5-85 : MC Link to Imported Firmware

ドロップダウンメニューからファームウェアバージョンを選択してから、デバイス上のバージョンと異なる場合にファームウェアを上書きするのか、テキスト入力フィールドに入力したファームウェアバージョンよりも前のバージョンの場合にファームウェアを上書きするのかを選択します。最後に **Select** をクリックします。

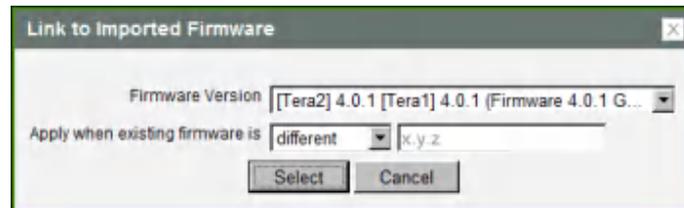


図 5-86 : MC Link to Imported Firmware - 設定後

表 5-80 : MC Link to Imported Firmware パラメータ

パラメータ	説明
Firmware Version	プロファイルに割り当てるファームウェアファイルを選択します。 注意：先に、 Update > Import Firmware メニューからファームウェアファイルを MC にインポートしておく必要があります。詳細については、『 PCoIP Management Console User Manual 』（TER0812002）を参照してください。
Apply when existing firmware is	ドロップダウンメニューから次のオプションのいずれかを設定します。 <ul style="list-style-type: none"> • different : このオプションは、デバイス上のファームウェアのバージョンが選択したバージョンと違っていればファームウェアを上書きする場合に選択します。 • less than : このオプションは、デバイス上のファームウェアのバージョンが x.y.z フィールド内のバージョンよりも前のバージョンであればファームウェアを上書きする場合に選択し、このフィールドにバージョンを入力します（4.0.2 など）。

5.23.2 AWI : ファームウェアアップロード設定

Firmware ページでは、新しいファームウェアビルドをホストまたはクライアントにアップロードすることができます。このページは、**Upload > Firmware** メニューからアクセスすることができます。

注意：ホストとクライアントに同じファームウェアリリースバージョンがインストールされている必要があります。

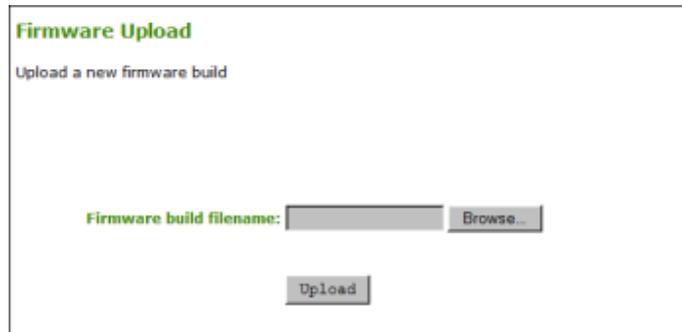


図 5-87 : AWI Firmware Upload ページ

表 5-81 : AWI Firmware Upload ページパラメータ

パラメータ	説明
Firmware build filename	アップロードするファームウェアイメージのファイル名。 Browse ボタンを使用してファイルを参照することができます。ファイルはウェブブラウザからアクセスできる必要があります（つまり、ローカルドライブまたはアクセス可能なネットワークドライブ上に存在する必要があります）。ファームウェアイメージは、".all"ファイルにする必要があります。
Upload	Upload ボタンをクリックすると指定されたファイルがデバイスに転送されます。偶発的なアップロードを避けるために、AWI からこの操作の確認が促されます。 注意 ：ホストとクライアントの両方に同じファームウェアリリースが存在することを保証することが重要です。

クライアントにファームウェアリリースをアップロードするには：

1. クライアントの AWI にログインします。
2. **Firmware Upload** ページで、ファームウェアファイルが格納されているフォルダを参照します。このファイルには、".all" 拡張子が付加されます。
3. 正しい "*.all" ファームウェアファイルをダブルクリックします。
4. **Upload** をクリックします。
5. **OK** をクリックしてアップロードの実行を確定します。この処理に数分かかる場合があります。完了すると、AWI ページに **Reset** と **Continue** の 2 つのボタンが表示されます。
6. **Reset** をクリックします。
7. **OK** をクリックします。

ホストにファームウェアリリースをアップロードするには：

1. ホスト PC またはワークステーションがアイドル状態になっている（つまり、すべてのアプリケーションが閉じている）ことを確認します。

2. ホストの AWI にログインします。
3. **Firmware Upload** ページで、ファームウェアファイルが格納されているフォルダを参照します。このファイルには、".all" 拡張子が付加されます。
4. 正しい "*.all" ファームウェアファイルをダブルクリックします。
5. **Upload** をクリックします。
6. **OK** をクリックしてアップロードの実行を確定します。この処理に数分かかる場合があります。完了すると、AWI ページに **Reset** と **Continue** の 2 つのボタンが表示されます。
7. **Reset** をクリックします。
8. **OK** をクリックします。
9. ホスト PC またはワークステーションの電源を入れ直します。ホストカードに変更を反映させるためには、PC またはワークステーションの電源オフ（再起動だけでなく）が必要です。

5.24 USB 承認の設定

5.24.1 MC : USB 承認

Profile Zero Client USB セクションは、管理コンソールの **Manage Profiles** ページの下部に配置されています。このセクションでは、クライアント上で設定された USB 設定を保持したり、その設定を無効にしたり、新しい設定を追加したりするようにプロファイルを構成することができます。

注意：USB Enhanced Host Controller Interface (EHCI) モードは、管理コンソールの [MC Peripheral Configuration](#) ページで設定します。

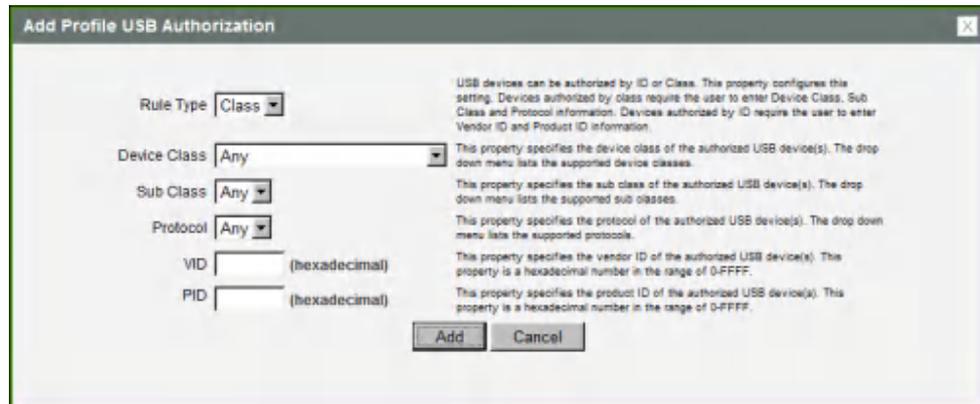
<input type="checkbox"/> Profile Zero Client USB Authorization	
Supported Device Family : ALL	
<input checked="" type="radio"/> Do not erase the device's existing USB authorizations	
<input type="radio"/> Erase the device's existing USB authorizations and replace them with an empty set	
Add New	
<input type="checkbox"/> Profile Zero Client USB Unauthorization	
Supported Device Family : ALL	
<input checked="" type="radio"/> Do not erase the device's existing USB unauthorizations	
<input type="radio"/> Erase the device's existing USB unauthorizations and replace them with an empty set	
Add New	
<input type="checkbox"/> Profile Zero Client USB Bridged	
Supported Device Family : ALL	
<input checked="" type="radio"/> Do not erase the device's existing USB bridged settings	
<input type="radio"/> Erase the device's existing USB bridged settings and replace them with an empty set	
Add New	

図 5-88 : MC プロファイルゼロクライアント USB 設定

表 5-82 : MC プロファイルゼロクライアント USB 設定パラメータ

パラメータ	説明
Profile Zero Client USB Authorization	<p>次のいずれかを選択します。</p> <ul style="list-style-type: none"> • Do not erase the device's existing USB authorizations : このオプションは、クライアント上で設定された既存の USB 許可設定を使用する場合に選択します。 • Erase the device's existing USB authorizations and replace them with an empty set : このオプションは、クライアント上で設定されたすべての USB 許可設定を削除する場合に選択します。 • Add New : このリンクは、クライアント上で設定された既存の設定に新しい USB 許可エントリを追加する場合にクリックします。
Profile Zero Client USB Unauthorization	<p>次のいずれかを選択します。</p> <ul style="list-style-type: none"> • Do not erase the device's existing USB unauthorizations : このオプションは、クライアント上で設定された既存の USB 非許可設定を使用する場合に選択します。 • Erase the device's existing USB unauthorizations and replace them with an empty set : このオプションは、クライアント上で設定されたすべての USB デバイスを無効にする場合に選択します。 • Add New : このリンクは、クライアント上で設定された既存の非許可設定に新しい USB 非許可エントリを追加する場合にクリックします。
Profile Zero Client USB Bridged	<p>次のいずれかを選択します。</p> <ul style="list-style-type: none"> • Do not erase the device's existing USB bridged settings : このオプションは、クライアント上で設定された既存の USB ブリッジ設定を使用する場合に選択します。 • Erase the device's existing USB bridged settings and replace them with an empty set : このオプションは、クライアント上で設定されたすべての USB ブリッジ設定を無効にする場合に選択します。 • Add New : このリンクは、クライアント上で設定された既存の設定に新しい USB ブリッジエントリを追加する場合にクリックします。

USB 許可、非許可、またはブリッジエントリの **Add New** をクリックした場合は、それぞれ、以下の画面が表示されます。



Add Profile USB Authorization

Rule Type:

Device Class:

Sub Class:

Protocol:

VID: (hexadecimal)

PID: (hexadecimal)

Buttons:

USB devices can be authorized by ID or Class. This property configures this setting. Devices authorized by class require the user to enter Device Class, Sub Class and Protocol information. Devices authorized by ID require the user to enter Vendor ID and Product ID information.

This property specifies the device class of the authorized USB device(s). The drop down menu lists the supported device classes.

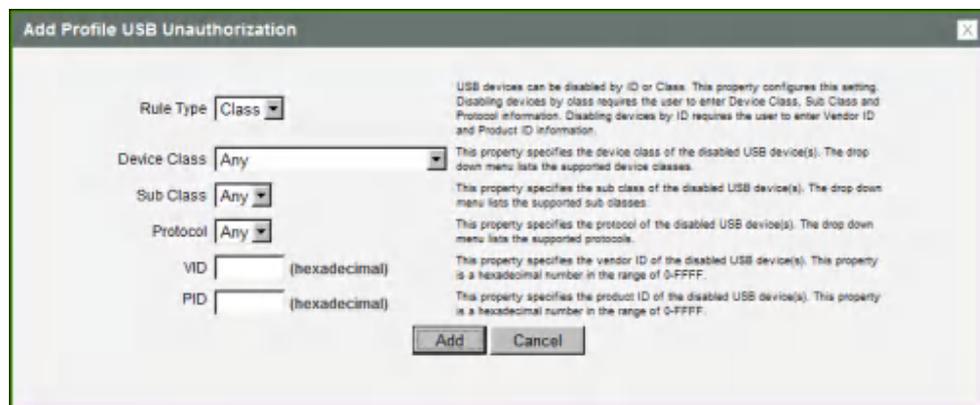
This property specifies the sub class of the authorized USB device(s). The drop down menu lists the supported sub classes.

This property specifies the protocol of the authorized USB device(s). The drop down menu lists the supported protocols.

This property specifies the vendor ID of the authorized USB device(s). This property is a hexadecimal number in the range of 0-FFFF.

This property specifies the product ID of the authorized USB device(s). This property is a hexadecimal number in the range of 0-FFFF.

図 5-89 : USB 許可 – Add New



Add Profile USB Unauthorization

Rule Type:

Device Class:

Sub Class:

Protocol:

VID: (hexadecimal)

PID: (hexadecimal)

Buttons:

USB devices can be disabled by ID or Class. This property configures this setting. Disabling devices by class requires the user to enter Device Class, Sub Class and Protocol information. Disabling devices by ID requires the user to enter Vendor ID and Product ID information.

This property specifies the device class of the disabled USB device(s). The drop down menu lists the supported device classes.

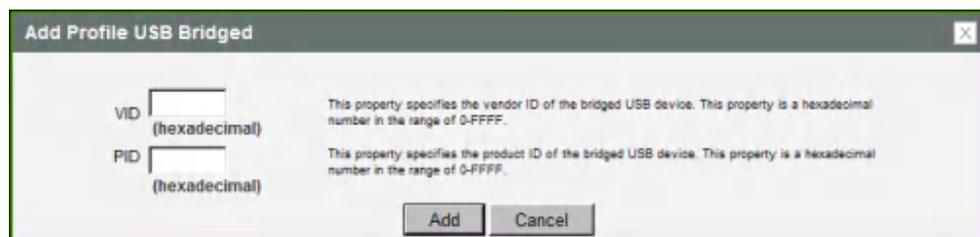
This property specifies the sub class of the disabled USB device(s). The drop down menu lists the supported sub classes.

This property specifies the protocol of the disabled USB device(s). The drop down menu lists the supported protocols.

This property specifies the vendor ID of the disabled USB device(s). This property is a hexadecimal number in the range of 0-FFFF.

This property specifies the product ID of the disabled USB device(s). This property is a hexadecimal number in the range of 0-FFFF.

図 5-90 : USB 非許可 – Add New



Add Profile USB Bridged

VID: (hexadecimal)

PID: (hexadecimal)

Buttons:

This property specifies the vendor ID of the bridged USB device. This property is a hexadecimal number in the range of 0-FFFF.

This property specifies the product ID of the bridged USB device. This property is a hexadecimal number in the range of 0-FFFF.

図 5-91 : USB ブリッジ – Add New

表 5-83 : Add Profile USB – Add New パラメータ

パラメータ	説明
Rule Type	新しい USB 許可または非許可エントリを追加するときに、次のいずれかを選択します。 <ul style="list-style-type: none"> • Class : USB デバイスはそのデバイスクラス、サブクラス、およびプロトコル情報によって許可されます。 • ID : USB デバイスはそのベンダ ID と製品 ID 情報によって許可されます。

パラメータ	説明
Device Class	このフィールドは、 Class が選択されたときに有効になります。 ド롭ダウンメニューからサポートされているデバイスクラスを選択するか、任意のデバイスクラスを許可または非許可（無効に）する場合は Any を選択します。
Sub Class	このフィールドは、 Class が選択されたときに有効になります。 ド롭ダウンメニューからサポートされているデバイスサブクラスを選択するか、任意のサブクラスを許可または非許可（無効に）する場合は Any を選択します。 注意 ：デバイスクラスとして Any を選択した場合は、これが唯一の使用可能な選択肢になります。
Protocol	このフィールドは、 Class が選択されたときに有効になります。 ド롭ダウンメニューからサポートされているプロトコルを選択するか、 Any を選択します。 注意 ：デバイスクラスまたはサブクラスとして Any を選択した場合は、これが唯一の使用可能な選択肢になります。
VID	このフィールドは、 ID が選択された場合、または、新しい USB ブリッジエントリを追加している場合に有効になります。 許可デバイス、非許可デバイス、またはブリッジデバイスのベンダ ID を入力します。有効範囲は 16 進数の 0~FFFF です。
PID	このフィールドは、 ID が選択された場合、または、新しい USB ブリッジエントリを追加している場合に有効になります。 許可デバイス、非許可デバイス、またはブリッジデバイスの製品 ID を入力します。有効範囲は 16 進数の 0~FFFF です。

5.24.2 AWI クライアント : USB 承認

USB ページは、**Permissions > USB** メニューからアクセスします。このページでは、ID またはクラスに基づいて、「ホワイトリスト」の USB デバイスを許可したり、「ブラックリスト」の USB デバイスを非許可したりすることができます。ワイルドカードを使用（または"any"を指定）して、すべてのデバイスの定義に必要なエントリ数を減らすことができます。

ホストにブリッジする必要があるデバイスを設定したり、特定の USB デバイスの USB 2.0 Enhanced Host Controller Interface (EHCI) モードを有効にしたりすることもできます。

非許可 USB デバイスの PCoIP ゼロクライアントハードウェアでは、USB プラグイベントがブロックされます。ホスト (PCoIP ホストカードまたはホスト仮想デスクトップ) では追加のセキュリティレイヤ用のデバイスを表示したり、それにアクセスしたりすることはできません。

USB ページはホストとクライアントの両方で使用できますが、ホスト **USB** 承認の方がクライアント **USB** 承認よりも優先されます。PCoIP ホストカードに接続する場合は、**USB** 承認をホスト上でのみ設定することを強くお勧めします。次のルールが適用されます。

- ホストで承認（許可または非許可）が設定されている場合は、その承認がクライアントに送信されます。クライアントで非許可デバイスが設定されている場合は、それらがホストの非許可デバイスに追加され、統合されたリストが使用されます。
- ホストで承認が設定されていない場合は、クライアントの承認が使用されます。

工場出荷時設定にはホスト上の **USB** 承認設定が含まれません。クライアント **USB** 承認の工場出荷時設定は"any、any、any"（つまり、許可 **USB** デバイス）です。ホスト実装（ハードウェア PCoIP ホストやソフトウェア PCoIP ホストなど）によっては、必要に応じて、クライアントまたはホスト上で **USB** 承認を設定することができます。

ホスト **USB** 承認は、PCoIP セッションの開始時点でのみ更新されます。これらは次の優先順位に従って許可されます（最高から最低の順）。

- 非許可ベンダ ID/製品 ID
- 許可ベンダ ID/製品 ID
- 非許可デバイスクラス/サブクラス/プロトコル
- 許可デバイスクラス/サブクラス/プロトコル



図 5-92 : AWI クライアント **USB** ページ

表 5-84 : AWI クライアント **USB** ページパラメータ

パラメータ	説明
Authorized Devices	デバイスの許可 USB デバイスを指定します。 Add New : 新しいデバイスまたはデバイスグループをリストに追加します。こ

パラメータ	説明
	<p>れにより、ID またはクラスによる USB 許可が可能になります。</p> <ul style="list-style-type: none"> • ID : USB デバイスはそのベンダ ID と製品 ID によって許可されます。 • Class : USB デバイスがデバイスクラス、サブクラス、およびプロトコルによって許可されます。 <p>Remove : デバイスまたはデバイスグループに関するルールをリストから削除します。</p>
Unauthorized Devices	<p>デバイスの非許可 USB デバイスを指定します。</p> <p>Add New : 新しいデバイスまたはデバイスグループをリストに追加します。これにより、ID またはクラスによる USB デバイスの非許可が可能になります。</p> <ul style="list-style-type: none"> • ID : USB デバイスはそのベンダ ID と製品 ID によって非許可されます。 • Class : USB デバイスがデバイスクラス、サブクラス、およびプロトコルによって非許可されます。 <p>Remove : デバイスまたはデバイスグループに関するルールをリストから削除します。</p>
Bridged Devices	<p>PCoIP ゼロクライアントは、VMware View 仮想デスクトップに接続するときに HID デバイスをローカルに終端します。ただし、デバイスによっては、HID としてアダプタイズしながら、別のドライバを使用している場合があります。このようなデバイスはローカルに終端するのではなく、ホストにブリッジする必要があります。この設定では、特定の USB デバイスをブリッジして仮想デスクトップ上のドライバを使用できるようにゼロクライアントに指示することができます。</p> <p>Add New : 新しいデバイスまたはデバイスグループをリストに追加します。これにより、ベンダ ID と製品 ID による USB デバイスのブリッジが可能になります。</p> <p>Remove : デバイスまたはデバイスグループに関するルールをリストから削除します。</p> <p>注意：ブリッジングはファームウェア 3.3.0 以降でサポートされている機能です。このルールは、ゼロクライアントと、VMware View 4.6 以降を実行しているソフトホスト間のセッションにのみ影響を与えます。</p>
Enable EHCI (root port only)	<p>このフィールドは、VMware View 4.6 以降を実行しているホストとのセッション用のゼロクライアント USB ポートに直接接続されたデバイスの EHCI (USB 2.0) を設定する場合に有効にします。</p> <p>注意：RAM が 128MB 未満のクライアント上では、この機能を有効にすることができません。等時性エンドポイントを備えたデバイスは USB 2.0 の速度で動作しません。</p>

新しい USB 許可エントリまたは非許可エントリを追加するときに、デバイスをクラスと ID のどちらで記述するかによって次のパラメータが表示されます。

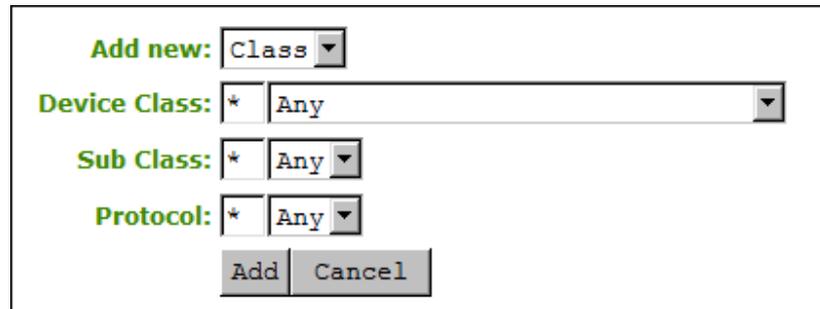


図 5-93 : デバイスクラスパラメータ

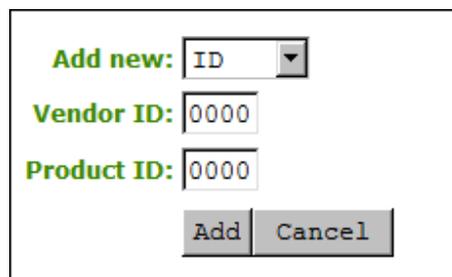


図 5-94 : デバイス ID パラメータ

表 5-85 : USB 許可/非許可デバイスパラメータ

パラメータ	説明
Add new	新しい USB 許可または非許可エントリを追加するときに、次のいずれかを選択します。 <ul style="list-style-type: none"> • Class : USB デバイスはそのデバイスクラス、サブクラス、およびプロトコル情報によって許可されます。 • ID : USB デバイスはそのベンダ ID と製品 ID 情報によって許可されます。
Device Class	このフィールドは、 Class が選択されたときに有効になります。 ドロップダウンメニューからサポートされているデバイスクラスを選択するか、任意のデバイスクラスを許可または非許可（無効に）する場合は Any を選択します。
Sub Class	このフィールドは、 Class が選択されたときに有効になります。 ドロップダウンメニューからサポートされているデバイスサブクラスを選択するか、任意のサブクラスを許可または非許可（無効に）する場合は Any を選択します。 注意：デバイスクラスとして Any を選択した場合は、これが唯一の使用可能な選択肢になります。
Protocol	このフィールドは、 Class が選択されたときに有効になります。 ドロップダウンメニューからサポートされているプロトコルを選択するか、 Any を選択します。

パラメータ	説明
	注意：デバイスクラスまたはサブクラスとして Any を選択した場合は、これが唯一の使用可能な選択肢になります。
Vendor ID	このフィールドは、 ID が選択されたときに有効になります。 許可（または非許可）デバイスのベンダ ID を入力します。有効範囲は 16 進数の 0~FFFF です。
Protocol ID	このフィールドは、 ID が選択されたときに有効になります。 (許可または非許可) デバイスの製品 ID を入力します。有効範囲は 16 進数の 0~FFFF です。

新しい USB ブリッジエントリを追加するときに、次のパラメータが表示されます。

図 5-95 : USB ブリッジパラメータ

表 5-86 : USB ブリッジデバイスパラメータ

パラメータ	説明
Vendor ID	ブリッジデバイスのベンダ ID を入力します。有効範囲は 16 進数の 0~FFFF です。
Protocol ID	ブリッジデバイスの製品 ID を入力します。有効範囲は 16 進数の 0~FFFF です。

5.24.3 AWI ホスト : USB 承認

USB ページは、**Permissions > USB** メニューからアクセスします。このページでは、ID またはクラスに基づいて、「ホワイトリスト」の USB デバイスを許可したり、「ブラックリスト」の USB デバイスを非許可したりすることができます。ワイルドカードを使用（または"any"を指定）して、すべてのデバイスの定義に必要なエントリ数を減らすことができます。

非許可 USB デバイスの PCoIP ゼロクライアントハードウェアでは、USB プラグイベントがブロックされます。ホスト（PCoIP ホストカードまたはホスト仮想デスク

トップ) では追加のセキュリティレイヤ用のデバイスを表示したり、それにアクセスしたりすることはできません。

USB ページはホストとクライアントの両方で使用できますが、ホスト **USB** 承認の方がクライアント **USB** 承認よりも優先されます。PCoIP ホストカードに接続する場合は、**USB** 承認をホスト上でのみ設定することを強くお勧めします。次のルールが適用されます。

- ホストで承認（許可または非許可）が設定されている場合は、その承認がクライアントに送信されます。クライアントで非許可デバイスが設定されている場合は、それらがホストの非許可デバイスに追加され、統合されたリストが使用されます。
- ホストで承認が設定されていない場合は、クライアントの承認が使用されます。

工場出荷時設定にはホスト上の **USB** 承認設定が含まれません。クライアント **USB** 承認の工場出荷時設定は"**any、any、any**"（つまり、許可 **USB** デバイス）です。ホスト実装（ハードウェア PCoIP ホストやソフトウェア PCoIP ホストなど）によっては、必要に応じて、クライアントまたはホスト上で **USB** 承認を設定することができます。

ホスト **USB** 承認は、PCoIP セッションの開始時点でのみ更新されます。これらは次の優先順位に従って許可されます（最高から最低の順）。

- 非許可ベンダ ID/製品 ID
- 許可ベンダ ID/製品 ID
- 非許可デバイスクラス/サブクラス/プロトコル
- 許可デバイスクラス/サブクラス/プロトコル

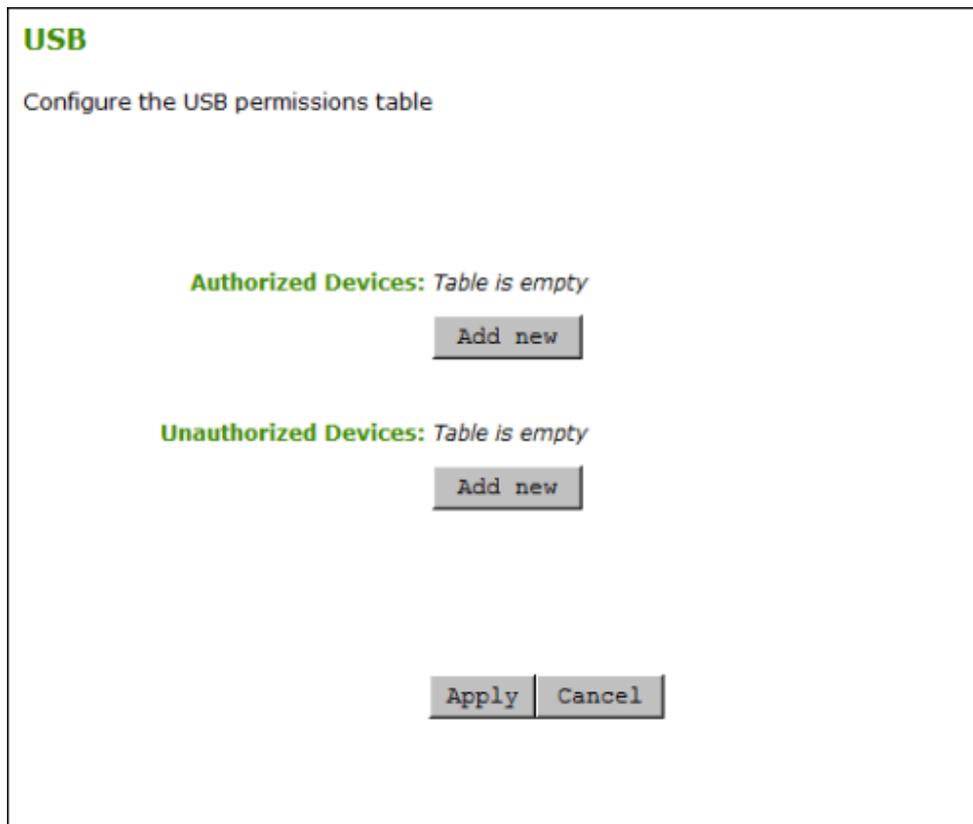


図 5-96 : AWI ホスト USB ページ

表 5-87 : AWI ホスト USB ページパラメータ

パラメータ	説明
Authorized Devices	<p>デバイスの許可 USB デバイスを指定します。</p> <p>Add New : 新しいデバイスまたはデバイスグループをリストに追加します。これにより、ID またはクラスによる USB 許可が可能になります。</p> <ul style="list-style-type: none"> • ID : USB デバイスがそのベンダ ID と製品 ID によって許可されます。 • Class : USB デバイスがデバイスクラス、サブクラス、およびプロトコルによって許可されます。 <p>Remove : デバイスまたはデバイスグループに関するルールをリストから削除します。</p>
Unauthorized Devices	<p>デバイスの非許可 USB デバイスを指定します。</p> <p>Add New : 新しいデバイスまたはデバイスグループをリストに追加します。これにより、ID またはクラスによる USB デバイスの非許可が可能になります。</p> <ul style="list-style-type: none"> • ID : USB デバイスがそのベンダ ID と製品 ID によって非許可されます。 • Class : USB デバイスがデバイスクラス、サブクラス、およびプロトコルによって非許可されます。 <p>Remove : デバイスまたはデバイスグループに関するルールをリストから削除</p>

パラメータ	説明
	します。

新しい USB 許可エントリまたは非許可エントリを追加するときに、デバイスをクラスと ID のどちらで記述するかによって次のパラメータが表示されます。

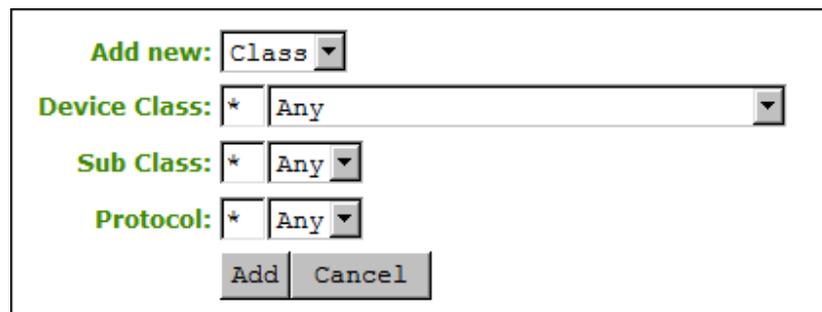


図 5-97 : デバイスクラスパラメータ

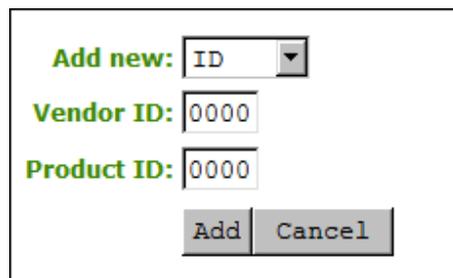


図 5-98 : デバイス ID パラメータ

表 5-88 : USB 許可/非許可デバイスパラメータ

パラメータ	説明
Add new	新しい USB 許可または非許可エントリを追加するときに、次のいずれかを選択します。 <ul style="list-style-type: none"> • Class : USB デバイスはそのデバイスクラス、サブクラス、およびプロトコル情報によって許可されます。 • ID : USB デバイスはそのベンダ ID と製品 ID 情報によって許可されます。
Device Class	このフィールドは、 Class が選択されたときに有効になります。 ドロップダウンメニューからサポートされているデバイスクラスを選択するか、任意のデバイスクラスを許可または非許可（無効に）する場合は Any を選択します。
Sub Class	このフィールドは、 Class が選択されたときに有効になります。

パラメータ	説明
	<p>ドロップダウンメニューからサポートされているデバイスサブクラスを選択するか、任意のサブクラスを許可または非許可（無効に）する場合は Any を選択します。</p> <p>注意：デバイスクラスとして Any を選択した場合は、これが唯一の使用可能な選択肢になります。</p>
Protocol	<p>このフィールドは、Class が選択されたときに有効になります。</p> <p>ドロップダウンメニューからサポートされているプロトコルを選択するか、Any を選択します。</p> <p>注意：デバイスクラスまたはサブクラスとして Any を選択した場合は、これが唯一の使用可能な選択肢になります。</p>
Vendor ID	<p>このフィールドは、ID が選択されたときに有効になります。</p> <p>許可（または非許可）デバイスのベンダ ID を入力します。有効範囲は 16 進数の 0~FFFF です。</p>
Protocol ID	<p>このフィールドは、ID が選択されたときに有効になります。</p> <p>（許可または非許可）デバイスの製品 ID を入力します。有効範囲は 16 進数の 0~FFFF です。</p>

5.25 証明書ストアの設定

5.25.1 MC：証明書ストア管理

Certificate Store セクションは、管理コンソールの **Manage Profiles** ページの下部に配置されています。このセクションでは、デバイス上で設定された証明書設定を保存したり、設定を無効にしたり、新しい証明書ファイルをプロファイルにアップロードしたりするようにプロファイルを構成することができます。

注意：最大 16 の証明書ファイルをプロファイルにアップロードして、それらの用途を設定することができます。

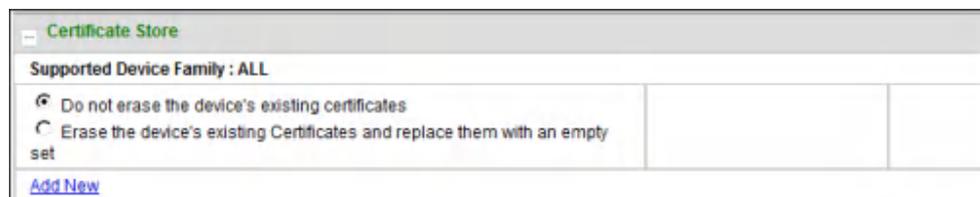


図 5-99：MC 証明書ストア設定

表 5-89：MC 証明書ストア設定パラメータ

パラメータ	説明

パラメータ	説明
Do not erase the device's existing certificates	このオプションは、プロファイルを通して、デバイス上で設定された既存の証明書設定を使用する場合に選択します。
Erase the device's existing Certificates and replace them with an empty set	このオプションは、プロファイルを通して、デバイス上で設定されたすべての証明書を無効にする場合に選択します。
Add New	新しい証明書ファイルをプロファイルにアップロードすることができます。

Add New をクリックすると、次の画面が表示されます。

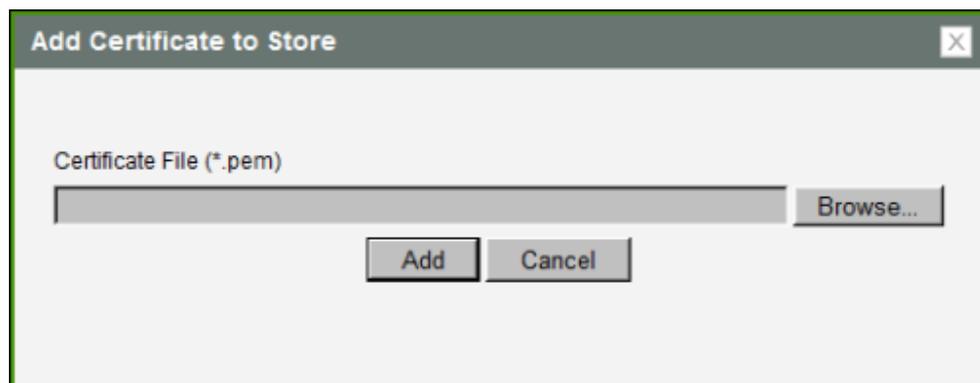


図 5-100 : MC Add Certificate to Store

表 5-90 : MC Add Certificate to Store パラメータ

パラメータ	説明
Certificate File (*.pem)	<p>Browse ボタンを使用して証明書ファイルを探してから、Add をクリックします。</p> <p>注意：最大 16 の証明書ファイルをプロファイルに追加することができます。</p>

証明書ファイルを追加したら、**Certificate Store** セクションにあるドロップダウンメニューから用途を選択することができます。

Certificate Store		
Supported Device Family : ALL		
Subject: DigiCert High Assurance EV Root CA Issued By: DigiCert High Assurance EV Root CA Expiration Date: 11/09/2031 Contains Private Key: False	No Usage ▾	Delete
Subject: 8021x-WIN-80AOGYIG8I3-CA Issued By: 8021x-WIN-80AOGYIG8I3-CA Expiration Date: 06/14/2016 Contains Private Key: False	No Usage ▾	Delete
Subject: Users Issued By: 8021x-WIN-80AOGYIG8I3-CA Expiration Date: 06/25/2013 Contains Private Key: True	No Usage ▾	Delete
Add New		

図 5-101 : MC Certificate Store

5.25.2 AWI : 証明書アップロード設定

Certificate Upload ページでは、CA ルート証明書とクライアント証明書をアップロードして管理することができます。このページは、**Upload > Certificate** メニューからアクセスすることができます。

注意 : 最大 16 の証明書をアップロードすることができます。ファームウェアリリース 3.5 現在、PCoIP プロトコルでは、802.1X 準拠ネットワーク用の 802.1X クライアント証明書が 1 つしか読み取られません。そのクライアント証明書に PCoIP デバイスに関するすべてのセキュリティ情報が含まれていることを確認してください。

802.1X 認証を使用する場合の一般的なガイドラインを以下に示します。詳細については、[Teradici サポートサイト](#) で知識ベースサポートトピック 15134-1063 を参照してください。

- 802.1X 認証には、802.1X クライアント証明書と 802.1X サーバ CA ルート証明書の 2 つの証明書が必要です。
- 802.1X クライアント証明書は、.pem 形式で作成し、RSA 暗号化を使用する秘密鍵を含める必要があります。証明書が別の形式の場合は、それをアップロードする前に、秘密鍵を含む.pem 形式に変換する必要があります。
- **Certificate Upload** ページで 802.1X クライアント証明書をアップロードしたら、[Network](#) ページで 802.1X 認証を設定する必要があります。このとき、802.1X 認証を有効にして、ゼロデバイスの識別文字列を入力し、ドロップダウンリストから正しい 802.1X クライアント証明書を選択してから、設定を適用する必要があります。
- 802.1X サーバ CA ルート証明書は、.pem 形式にする必要がありますが、秘密鍵を含める必要はありません。証明書が別の形式の場合は、それをアップロードする前に、.pem 形式に変換する必要があります。この証明書の場合は、**Network** ページでの設定が必要ありません。
- 802.1X クライアント証明書と 802.1X サーバ CA ルート証明書はどちらも 6 KB 未満にする必要があります。そうしなければ、アップロードすることができません。証明書ファイルによっては複数の証明書が含まれている場合があります。証明書ファイルが大き過ぎて、複数の証明書が含まれている場合は、そのファイルをテ

キストエディタで開いて、個別の証明書をコピーして別々のファイルに保存することができます。



図 5-102 : AWI Certificate Upload ページ

表 5-91 : AWI Certificate Upload ページパラメータ

パラメータ	説明
Certificate filename	最大 16 のルート証明書とクライアント証明書をアップロードします。
Uploaded Certificates	アップロード済みの証明書が表示されます。アップロード済みの証明書を削除するには、 Remove ボタンをクリックします。削除プロセスはデバイスの再起動後に行われます。証明書の詳細を確認するには、 Detail ボタンをクリックします。これらの証明書が Network ページの Client Certificate ドロップダウンメニュー内のオプションとして表示されます。
802.1X Client Certificate	読み取り専用フィールドです。 Network ページの Client Certificate フィールドにリンクされています。

5.26 OSD ディスプレイオーバーライドの設定

5.26.1 OSD デュアルディスプレイ : ディスプレイ設定

Display ページでは、拡張ディスプレイ識別データ (EDID) オーバーライドモードを有効にすることができます。

注意 : この機能は OSD 経由でしか使用することができません。

通常の操作では、ホストコンピュータ内の GPU がモニタの機能を特定するためにモニタをゼロクライアントに接続する必要があります。モニタの機能は EDID 情報として報告されます。状況によっては、特定の KVM デバイス経由で接続されている場合のように、クライアントが EDID 情報を読み取れない形態でモニタがクライアントに接続されている場合があります。このページの **Preferred Resolution Override**

機能を使用すれば、デフォルト EDID 情報を GPU にアドバタイズするようにクライアントを設定することができます。

警告： Preferred Resolution Override 機能は、有効な EDID 情報が存在せず、モニタのディスプレイ特性が認識されている場合にのみ有効にする必要があります。EDID の読み取りに失敗する場合は、ドロップダウンリストにディスプレイでサポートされていない解像度が含まれている可能性があります。ディスプレイに何も映らない場合、または、優先解像度を設定後に「Timing Out of Range」というメッセージが 30 秒以上表示された場合は、ビデオケーブルを抜き差ししてディスプレイの解像度を以前の値に戻すことができます。

注意： TERA2321 ゼロクライアントデバイスをクライアントとして使用している場合は、このページに 2 つのモニタに関する優先解像度設定しか表示されません。

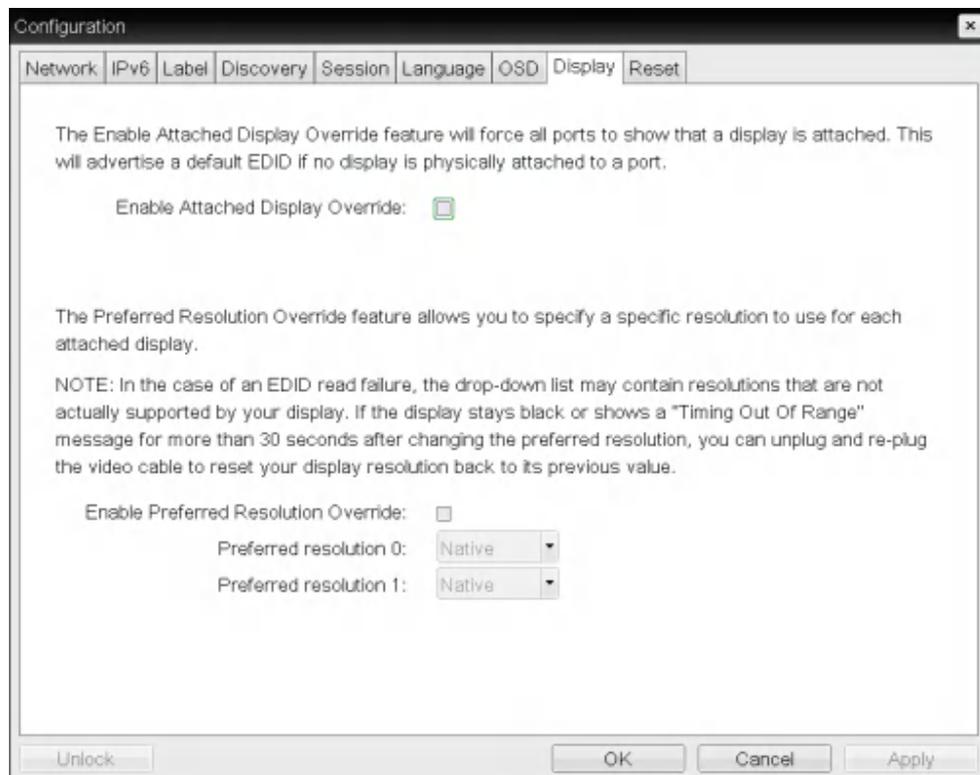


図 5-103 : OSD Tera1Display ページ

表 5-92 : OSD Tera1 Display ページパラメータ

パラメータ	説明
Enable Attached Display Override	このオプションはレガシーシステム用です。モニタが検出できない場合やモニタがクライアントに接続されていない場合に、デフォルト EDID 情報をホストに送信するようにクライアントが設定されます。Windows のバージョンが Windows 7 より前の場合は、ホストに EDID 情報が存在しなければ、モニタが接続されていないと判断され、二度とチェックが行われません。このオプションは、クライアント

パラメータ	説明
	<p>トがセッション中は必ずホストに EDID 情報が存在することを保証します。</p> <p>このオプションが有効になっている場合は、以下のデフォルト解像度がアダプタイズされます。</p> <ul style="list-style-type: none"> • 2560x1600 @60 Hz • 2048x1152 @60 Hz • 1920x1440 @60 Hz • 1920x1200 @60 Hz • 1920x1080 @60 Hz • 1856x1392 @60 Hz • 1792x1344 @60 Hz • 1680x1050 @60 Hz • 1600x1200 @60 Hz • 1600x900 @60 Hz • 1440x900 @60 Hz • 1400x1050 @60 Hz • 1366x768 @60 Hz • 1360x768 @60 Hz • 1280x1024 @60 Hz • 1280x960 @60 Hz • 1280x800 @60 Hz • 1280x768 @60 Hz • 1280x720 @60 Hz • 1024x768 @60 Hz • 848x480 @60 Hz • 800x600 @60 Hz • 640x480 @60 Hz <p>このオプションが有効になっている場合は、クライアントに接続されたすべてのディスプレイがネイティブ解像度の 1024x768 に設定されます。</p>
Enable Preferred Resolution Override	<p>このオプションは、ディスプレイが接続されているがシステムで検出できないため、ディスプレイの優先解像度を指定したい場合に有効にします。デフォルトネイティブ解像度の 1024x768 の代わりに、ここでディスプレイに対して設定された優先解像度がネイティブ解像度として送信される場合を除いて、上記と同じデフォルト解像度リストがアダプタイズされます。</p> <ul style="list-style-type: none"> • Preferred resolution 0 : ゼロクライアントのポート 1 に接続されたディスプレイの優先解像度を選択します。 • Preferred resolution 1 : ゼロクライアントのポート 2 に接続されたディスプレイの優先解像度を選択します。 <p>このオプションが有効になっている場合は、クライアントに接続されたすべてのディスプレイが、指定された優先解像度に設定されます。</p>

5.26.2 OSD クアッドディスプレイ：ディスプレイ設定

Display ページでは、拡張ディスプレイ識別データ (EDID) オーバーライドモードを有効にすることができます。

注意：この機能は OSD 経由でしか使用することができません。

通常の操作では、ホストコンピュータ内の GPU がモニタの機能を特定するためにモニタをゼロクライアントに接続する必要があります。モニタの機能は EDID 情報として報告されます。状況によっては、特定の KVM デバイス経由で接続されている場合のように、クライアントが EDID 情報を読み取れない形態でモニタがクライアントに接続されている場合があります。このページの **Preferred Resolution Override** 機能を使用すれば、デフォルト EDID 情報を GPU にアダプタイズするようにクライアントを設定することができます。

警告：Preferred Resolution Override 機能は、有効な EDID 情報が存在せず、モニタのディスプレイ特性が認識されている場合にのみ有効にする必要があります。EDID の読み取りに失敗する場合は、ドロップダウンリストにディスプレイでサポートされていない解像度が含まれている可能性があります。ディスプレイに何も映らない場合、または、優先解像度を設定後に「Timing Out of Range」というメッセージが 30 秒以上表示された場合は、ビデオケーブルを抜き差ししてディスプレイの解像度を以前の値に戻すことができます。

注意：TERA2321 ゼロクライアントデバイスをクライアントとして使用している場合は、[ここ](#)に示すように、このページに 2 つのモニタに関する優先解像度設定しか表示されません。

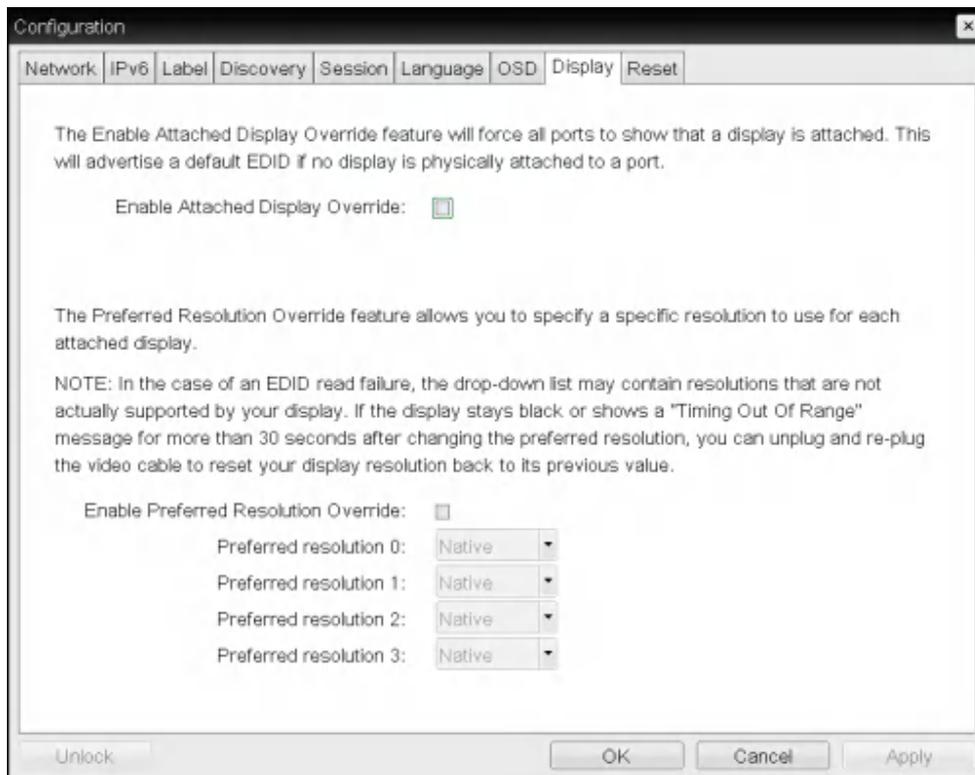


図 5-104 : OSD Tera2 Display ページ

表 5-93 : OSD Tera2 Display ページパラメータ

パラメータ	説明
Enable Attached Display Override	<p>このオプションはレガシーシステム用です。モニタが検出できない場合やモニタがクライアントに接続されていない場合に、デフォルト EDID 情報をホストに送信するようにクライアントが設定されます。Windows のバージョンが Windows 7 より前の場合は、ホストに EDID 情報が存在しなければ、モニタが接続されていないと判断され、二度とチェックが行われません。このオプションは、クライアントがセッション中は必ずホストに EDID 情報が存在することを保証します。</p> <p>このオプションが有効になっている場合は、以下のデフォルト解像度がアドバタイズされます。</p> <ul style="list-style-type: none"> • 2560x1600 @60 Hz • 2048x1152 @60 Hz • 1920x1440 @60 Hz • 1920x1200 @60 Hz • 1920x1080 @60 Hz • 1856x1392 @60 Hz • 1792x1344 @60 Hz • 1680x1050 @60 Hz • 1600x1200 @60 Hz

パラメータ	説明
	<ul style="list-style-type: none"> • 1600x900 @60 Hz • 1440x900 @60 Hz • 1400x1050 @60 Hz • 1366x768 @60 Hz • 1360x768 @60 Hz • 1280x1024 @60 Hz • 1280x960 @60 Hz • 1280x800 @60 Hz • 1280x768 @60 Hz • 1280x720 @60 Hz • 1024x768 @60 Hz • 848x480 @60 Hz • 800x600 @60 Hz • 640x480 @60 Hz <p>このオプションが有効になっている場合は、クライアントに接続されたすべてのディスプレイがネイティブ解像度の 1024x768 に設定されます。</p>
<p>Enable Preferred Resolution Override</p>	<p>このオプションは、ディスプレイが接続されているがシステムで検出できないため、ディスプレイの優先解像度を指定したい場合に有効にします。デフォルトネイティブ解像度の 1024x768 の代わりに、ここでディスプレイに対して設定された優先解像度がネイティブ解像度として送信される場合を除いて、上記と同じデフォルト解像度リストがアドバタイズされます。</p> <ul style="list-style-type: none"> • Preferred resolution 0 : ゼロクライアントのポート 1 に接続されたディスプレイの優先解像度を選択します。 • Preferred resolution 1 : ゼロクライアントのポート 2 に接続されたディスプレイの優先解像度を選択します。 • Preferred resolution 2 : ゼロクライアントのポート 3 に接続されたディスプレイの優先解像度を選択します。 • Preferred resolution 3 : ゼロクライアントのポート 4 に接続されたディスプレイの優先解像度を選択します。 <p>このオプションが有効になっている場合は、クライアントに接続されたすべてのディスプレイが、指定された優先解像度に設定されます。</p>

5.27 パスワードとリセットパラメータの設定 (AWI/OSD)

5.27.1 AWI : パスワード設定

Password ページでは、デバイスのローカル管理パスワードを更新することができます。このページは、ホストまたはクライアントの **Configuration > Password** メニューからアクセスすることができます。

パスワードは 20 文字以下にする必要があります。PCoIP デバイスによってはデフォルトでパスワード保護が無効になっている場合があります、このようなデバイスでは **Password** ページが使用できません。MC の [Security Configuration](#) ページでこのようなデバイスのパスワード保護を有効にすることができます。

注意：このパラメータは AWI とローカル OSD GUI に影響を与えます。パスワードを忘れるとクライアントが使用できなくなるため、クライアントパスワードの更新は慎重に行ってください。

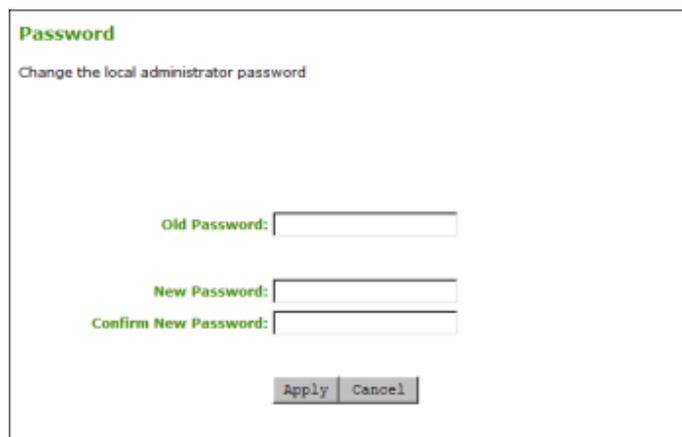


図 5-105 : AWI Password ページ

表 5-94 : AWI Password ページパラメータ

パラメータ	説明
Old Password	このフィールドが現在の管理パスワードと合っていない場合は、パスワードを更新することができません。
New Password	AWI とローカル OSD GUI の両方の新しい管理パスワード。
Confirm New Password	変更を実施するためには、このフィールドと New Password フィールドが一致している必要があります。

5.27.2 OSD : パスワード設定

Password ページでは、デバイスのローカル管理パスワードを更新することができます。このページは、**Options > Password** メニューからアクセスすることができます。

パスワードは 20 文字以下にする必要があります。PCoIP デバイスによってはデフォルトでパスワード保護が無効になっている場合があります、このようなデバイスでは **Password** ページが使用できません。MC の [Security Configuration](#) ページでこのようなデバイスのパスワード保護を有効にすることができます。

注意：このパラメータは AWI とローカル OSD GUI に影響を与えます。パスワードを忘れるとクライアントが使用できなくなるため、クライアントパスワードの更新は慎重に行ってください。

図 5-106 : OSD Change Password ページ

表 5-95 : OSD Change Password ページパラメータ

パラメータ	説明
Old Password	このフィールドが現在の管理パスワードと合っていないければ、パスワードを更新することができません。
New Password	AWI とローカル OSD GUI の両方の新しい管理パスワード。
Confirm New Password	変更を実施するためには、このフィールドと New Password フィールドが一致している必要があります。
Reset	クライアントパスワードを忘れた場合は、 Reset ボタンをクリックしてゼロクライアントベンダに応答コードを要求することができます。チャレンジコードがベンダに送信されます。ベンダは要求を吟味して、Teradici で許可された場合に、応答コードを返します。応答コードが正しく入力されれば、クライアントのパスワードが空の文字列にリセットされます。新しいパスワードを入力する必要があります。 注意：パスワードリセットの許可が必要な場合の詳細については、クライアントベンダにお問い合わせください。このオプションは AWI 経由では使用できません。OSD 経由でしか使用することができません。

5.27.3 AWI ホスト：パラメータリセット設定

Reset Parameters ページでは、設定と承認をフラッシュメモリに保存された工場出荷時設定値にリセットすることができます。このページは、**Configuration > Reset Parameters** メニューからアクセスすることができます。

注意：パラメータを工場出荷時設定値にリセットしてもファームウェアが元に戻されたり、カスタム OSD ロゴが消去されたりすることはありません。

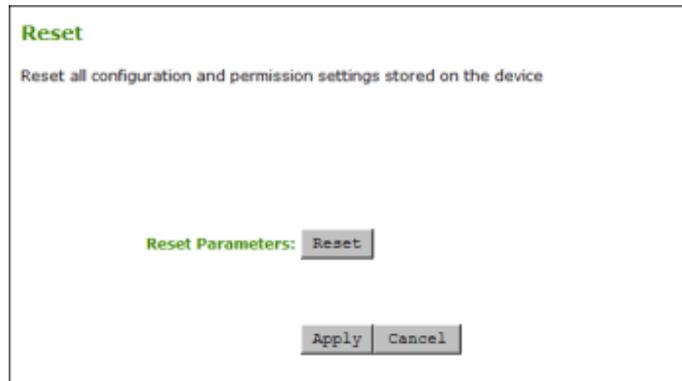


図 5-107 : AWI ホスト Reset ページ

表 5-96 : AWI ホスト Reset ページパラメータ

パラメータ	説明
Reset Parameters	このボタンをクリックすると、確認のためのプロンプトが表示されます。これは偶発的なリセットを防ぐためです。

5.27.4 AWI クライアント : パラメータリセット設定

Reset Parameters ページでは、設定と承認をフラッシュメモリに保存された工場出荷時設定値にリセットすることができます。このページは、**Configuration > Reset Parameters** メニューからアクセスすることができます。

注意：パラメータを工場出荷時設定値にリセットしてもファームウェアが元に戻されたり、カスタム OSD ロゴが消去されたりすることはありません。

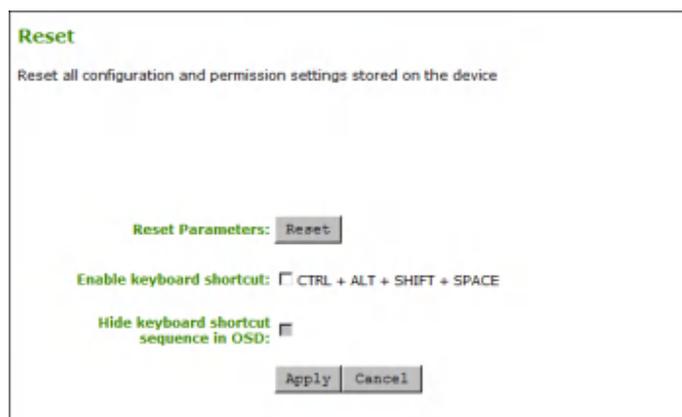


図 5-108 : AWI クライアント Reset ページ

表 5-97 : AWI クライアント Reset ページパラメータ

パラメータ	説明
-------	----

パラメータ	説明
Reset Parameters	このボタンをクリックすると、確認のためのプロンプトが表示されます。この目的は偶発的なリセットを防ぐためです。
Enable Keyboard Shortcut	有効になっている場合は、ユーザが指定されたキーの組み合わせを押すことで、デバイスのパラメータと承認を自動的にリセットすることができます。
Hide keyboard shortcut sequence in OSD	<p>Enable Keyboard Shortcut が有効になっており、このフィールドが無効になっている場合は、キーボードシーケンスがクライアントの Reset Parameters ページに表示されます。</p> <p>Enable Keyboard Shortcut フィールドとこのフィールドの両方が有効になっている場合は、キーボードシーケンスがクライアントの Reset Parameters ページに表示されませんが、ユーザはキーボードシーケンスを使用してパラメータをリセットすることができます。</p>

5.27.5 OSD : パラメータリセット設定

Reset ページでは、設定と承認をフラッシュメモリに保存された工場出荷時設定値にリセットすることができます。このページは、**Options > Configuration > Reset** メニューからアクセスすることができます。

注意：パラメータを工場出荷時設定値にリセットしてもファームウェアが元に戻されたり、カスタム OSD ロゴが消去されたりすることはありません。

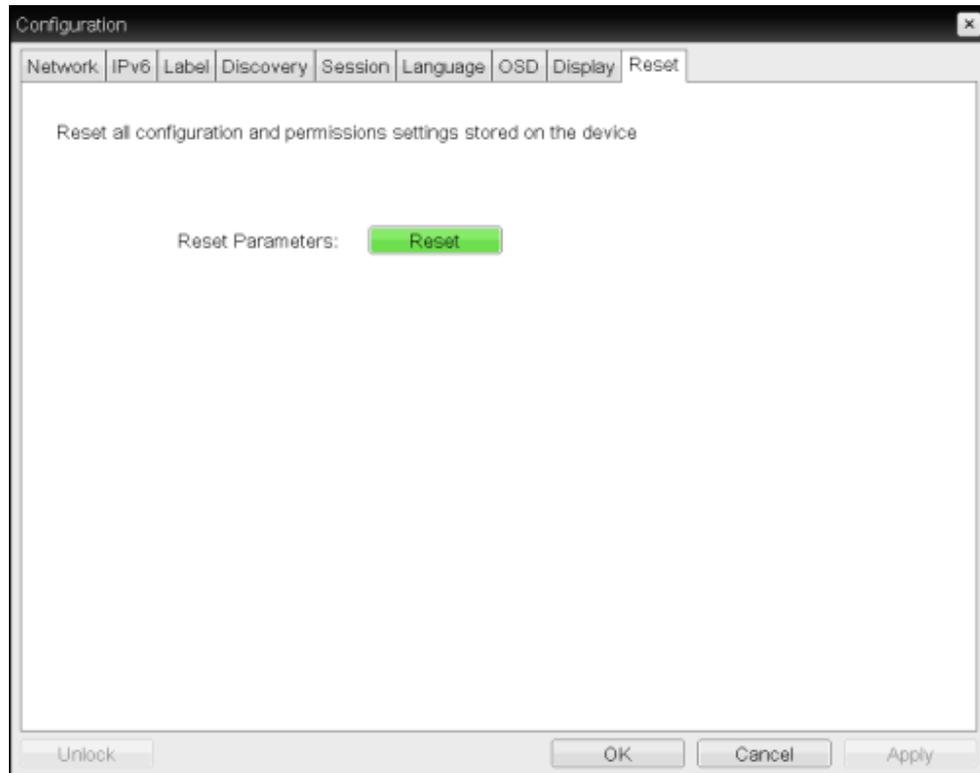


図 5-109 : OSD Reset ページ

表 5-98 : OSD Reset ページパラメータ

パラメータ	説明
Reset Parameters	このボタンをクリックすると、確認のためのプロンプトが表示されます。この目的は偶発的なリセットを防ぐためです。

5.28 診断の表示 (AWI/OSD)

5.28.1 AWI : イベントログ設定に関するヘルプ

AWI の **Event Log** ページの詳細については、「[AWI : イベントログ設定](#)」を参照してください。

5.28.2 OSD : イベントログ設定に関するヘルプ

OSD の **Event Log** ページの詳細については、「[OSD : イベントログ設定](#)」を参照してください。

5.28.3 AWI ホスト : セッション制御設定

Session Control ページでは、デバイスに関する情報を表示したり、セッションを手動で切断または接続したりすることができます。このページは、**Diagnostics > Session Control** メニューからアクセスすることができます。



図 5-110 : AWI ホスト Session Control ページ

表 5-99 : AWI ホスト Session Control ページパラメータ

パラメータ	説明
Connection State	<p>このフィールドにはセッションの現状が表示されます。次のようなオプションがあります。</p> <ul style="list-style-type: none">• Disconnected• Connection Pending• Connected <p>Connection State フィールドの下に次の 2 つのボタンが表示されます。</p> <ul style="list-style-type: none">• Connect : ホストではこのボタンが無効になっています。• Disconnect : 接続状態が Connected または Connection Pending の場合は、このボタンをクリックしてデバイスの PCoIP セッションを終了します。接続状態が Disconnected の場合は、このボタンが無効になります。
Peer IP	<p>Peer IP Address : ピアデバイスの IP アドレスが表示されます。セッション中以外は、このフィールドが空白になります。</p>
Peer MAC Address	<p>Peer MAC Address : ピアデバイスの MAC アドレスが表示されます。セッション中以外は、このフィールドが空白になります。</p>

5.28.4 AWI クライアント : セッション制御設定

Session Control ページでは、デバイスに関する情報を表示したり、セッションを手動で切断または接続したりすることができます。このページは、**Diagnostics > Session Control** メニューからアクセスすることができます。



図 5-111 : AWI クライアント Session Control ページ

表 5-100 : AWI クライアント Session Control ページパラメータ

パラメータ	説明
Connection State	<p>このフィールドにはセッションの現状が表示されます。次のようなオプションがあります。</p> <ul style="list-style-type: none"> • Disconnected • Connection Pending • Connected <p>Connection State フィールドの下に次の 2 つのボタンが表示されます。</p> <ul style="list-style-type: none"> • Connect : 接続状態が Disconnected の場合は、このボタンをクリックしてクライアントとピアデバイス間の PCoIP セッションを開始します。接続状態が Connection Pending または Connected の場合は、このボタンが無効になります。 • Disconnect : 接続状態が Connected または Connection Pending の場合は、このボタンをクリックしてデバイスの PCoIP セッションを終了します。接続状態が Disconnected の場合は、このボタンが無効になります。
Peer IP	<p>Peer IP Address : ピアデバイスの IP アドレスが表示されます。セッション中以外は、このフィールドが空白になります。</p>
Peer MAC Address	<p>Peer MAC Address : ピアデバイスの MAC アドレスが表示されます。セッション中以外は、このフィールドが空白になります。</p>

5.28.5 AWI ホスト : セッション統計情報設定

Session Statistics ページでは、セッションがアクティブな場合に最新の統計情報を表示することができます。セッションが非アクティブな場合は、最後のセッションの統計情報が表示されます。このページは、**Diagnostics > Session Statistics** メニューから表示することができます。

Session Statistics

View statistics for the current session

Connection State: Connected to TERA2140 client 192.168.54.133

802.1X Authentication Status: Disabled

PCoIP Packets (Sent/Received/Lost): 42885 / 28458 / 0

Bytes (Sent/Received): 19081850 / 3629012

Round Trip Latency (Min/Avg/Max): 2 / 2 / 5 ms

Transmit Bandwidth (Min/Avg/Max/Limit): 8 / 1240 / 5784 / 11568 kbps

Receive Bandwidth (Min/Avg/Max): 0 / 232 / 392 kbps

Pipeline Processing Rate (Avg/Max/Limit): 1 / 39 / 297 Mpps

Endpoint Image Settings In Use: Client

Initial Image Quality (Min/Active/Max): 40 / 90 / 90

Image Quality Preference: 50

Build To Lossless: Enabled

Display	Maximum Rate: Refresh Rate	Input Change Rate	Output Process Rate	Image Quality
1	60 fps	23 fps	21 fps	Perceptually Lossless
2	N/A	N/A	N/A	N/A
3	60 fps	0 fps	0 fps	Lossless
4	N/A	N/A	N/A	N/A

図 5-112 : AWI ホスト Session Statistics ページ

注意：上の図は、4 台のディスプレイが接続されたクライアントに接続されたホストカードに関するセッション統計情報を示しています。デプロイメントで 2 台のディスプレイが使用されている場合は、2 台のディスプレイに関する情報しかこのセッションに表示されません。

表 5-101 : AWI ホスト Session Statistics ページパラメータ

パラメータ	説明
Connection State	PCoIP セッションの現在（または最後）の状態。値には以下が含まれます。 <ul style="list-style-type: none"> • Asleep

パラメータ	説明
	<ul style="list-style-type: none"> • Canceling • Connected • Connection Pending • Disconnected • Waking
802.1X Authentication Status	デバイス上で 802.1X 認証が有効になっているか、無効になっているかを示します。
PCoIP Packets Statistics	<p>PCoIP Packets Sent : 現在/最後のセッションで送信された PCoIP パケットの総数。</p> <p>PCoIP Packets Received : 現在/最後のセッションで受信された PCoIP パケットの総数。</p> <p>PCoIP Packets Lost : 現在/最後のセッションで消失された PCoIP パケットの総数。</p>
Bytes	<p>Bytes Sent : 現在/最後のセッションで送信されたバイトの総数。</p> <p>Bytes Received : 現在/最後のセッションで受信されたバイトの総数。</p>
Round Trip Latency	PCoIP システムとネットワークの往復遅延の最小値、平均値、および最大値 (ミリ秒 (+/- 1 ms) 単位)
Bandwidth Statistics	<p>Transmit Bandwidth : Tera プロセッサによって送信された最小、平均、および最大トラフィック。有効帯域幅限界は Tera プロセッサが生成する可能性のあるネットワークトラフィックの最大量です。この値は、設定された帯域幅パラメータと現在 (または最後) のネットワーク混雑レベルから抽出されます。</p> <p>Receive Bandwidth : Tera プロセッサによって受信された最小、平均、および最大トラフィック。</p>
Pipeline Processing Rate	イメージエンジンによって現在処理されているイメージデータの容量 (メガピクセル数/秒単位)。
Endpoint Image Settings In Use	使用されているイメージ設定がクライアントで設定されたのか、ホストで設定されたのかを示します。これは、ホストデバイスの Image ページで Use Client Image Settings フィールドがどのように設定されているかに基づきます。
Initial Image Quality	<p>最低品質設定と最高品質設定はデバイスの Image ページから取得されます。</p> <p>アクティブ設定は現在セッションで使用されている設定で、ホスト上にもみ表示されます。</p>

パラメータ	説明
Image Quality Preference	この設定は、 Image ページの Image Quality Preference フィールドから取得されます。この値は、イメージがよりスムーズなイメージに設定されているのか、よりシャープなイメージに設定されているのかを示します。
Build to Lossless	このフィールドに表示されるオプションには以下が含まれます。 Enabled : Image ページの Disable Build to Lossless フィールドがオフになっています。 Disabled : Disable Build to Lossless フィールドがオンになっています。
Reset Statistics	このボタンをクリックすると、このページ上の統計情報がリセットされます。 注意 : Reset Statistics ボタンは、 Home ページで報告された統計情報もリセットします。
Display	ディスプレイのポート番号。
Maximum Rate	この列は取り付けられたディスプレイのリフレッシュレートを表します。 Image ページの Maximum Rate フィールドが 0 (つまり、無制限) に設定されている場合は、最大レートがモニタのリフレッシュレートから取得されます。 Image ページの Maximum Rate フィールドが 0 より大きい値に設定されている場合は、リフレッシュレートが "User Defined" として表示されます。
Input Change Rate	GPU からのコンテンツ変更率。これには、ユーザが実行しているすべてのもの (カーソル移動、電子メール編集、ストリーミングビデオなど) が含まれます。
Output Process Rate	ホスト上のイメージエンジンからクライアントに現在送信されているフレームレート。
Image Quality	取り付けられたディスプレイの現在のロスレス状態を示します。 <ul style="list-style-type: none"> • Lossy • Perceptually lossless • Lossless

5.28.6 AWI クライアント : セッション統計情報設定

Session Statistics ページでは、セッションがアクティブな場合に最新の統計情報を表示することができます。セッションが非アクティブな場合は、最後のセッションの

統計情報が表示されます。このページは、**Diagnostics > Session Statistics** メニューから表示することができます。

Session Statistics

View statistics for the current session

Connection State: Connected to host [192.168.65.103](#)

802.1X Authentication Status: Disabled

PCoIP Packets (Sent/Received/Lost): 44769 / 68244 / 0

Bytes (Sent/Received): 5638498 / 31681880

Round Trip Latency (Min/Avg/Max): 2 / 2 / 4 ms

Transmit Bandwidth (Min/Avg/Max/Limit): 8 / 112 / 392 / 8000 kbps

Receive Bandwidth (Min/Avg/Max): 0 / 200 / 5600 kbps

Pipeline Processing Rate (Avg/Max/Limit): 1 / 37 / 297 Mpps

Endpoint Image Settings In Use: Client

Initial Image Quality (Min/Max): 40 / 90

Image Quality Preference: 50

Build To Lossless: Enabled

Display	Maximum Rate: Refresh Rate	Output Process Rate	Image Quality
1	60 fps	8 fps	Lossy
2	60 fps	0 fps	Lossless
3	N/A	N/A	N/A
4	N/A	N/A	N/A

図 5-113 : AWI クライアント Session Statistics ページ

注意：上の図は、2 台のディスプレイが接続されたクライアントに関するセッション統計情報を示しています。デプロイメントで 4 台のディスプレイが使用されている場合は、4 台すべてのディスプレイに関する情報がこのセクションに表示されません。

表 5-102 : AWI クライアント Session Statistics ページパラメータ

パラメータ	説明
Connection State	PCoIP セッションの現在（または最後）の状態。値には以下が含まれます。 <ul style="list-style-type: none"> • Asleep

パラメータ	説明
	<ul style="list-style-type: none"> • Canceling • Connected • Connection Pending • Disconnected • Waking
802.1X Authentication Status	デバイス上で 802.1X 認証が有効になっているか、無効になっているかを示します。
PCoIP Packets Statistics	<p>PCoIP Packets Sent : 現在/最後のセッションで送信された PCoIP パケットの総数。</p> <p>PCoIP Packets Received : 現在/最後のセッションで受信された PCoIP パケットの総数。</p> <p>PCoIP Packets Lost : 現在/最後のセッションで消失された PCoIP パケットの総数。</p>
Bytes	<p>Bytes Sent : 現在/最後のセッションで送信されたバイトの総数。</p> <p>Bytes Received : 現在/最後のセッションで受信されたバイトの総数。</p>
Round Trip Latency	PCoIP システムとネットワークの往復遅延の最小値、平均値、および最大値 (ミリ秒 (+/- 1 ms) 単位)
Bandwidth Statistics	<p>Transmit Bandwidth : Tera プロセッサによって送信された最小、平均、および最大トラフィック。有効帯域幅限界は Tera プロセッサが生成する可能性のあるネットワークトラフィックの最大量です。この値は、設定された帯域幅パラメータと現在 (または最後) のネットワーク混雑レベルから抽出されます。</p> <p>Receive Bandwidth : Tera プロセッサによって受信された最小、平均、および最大トラフィック。</p>
Pipeline Processing Rate	イメージエンジンによって現在処理されているイメージデータの容量 (メガピクセル数/秒単位)
Endpoint Image Settings In Use	使用されているイメージ設定がクライアントで設定されたのか、ホストで設定されたのかを示します。これは、ホストデバイスの Image ページで Use Client Image Settings フィールドがどのように設定されているかに基づきます。
Initial Image Quality	最低品質設定と最高品質設定はデバイスの Image ページから取得されます。
Image Quality Preference	この設定は、 Image ページの Image Quality Preference フィールドから取得されます。この値は、イメージがよりスムーズなイメージに

パラメータ	説明
	設定されているのか、よりシャープなイメージに設定されているのかを示します。
Build to Lossless	このフィールドに表示されるオプションには以下が含まれます。 Enabled : Image ページの Disable Build to Lossless フィールドがオフになっています。 Disabled : Disable Build to Lossless フィールドがオンになっています。
Reset Statistics	このボタンをクリックすると、このページ上の統計情報がリセットされます。 注意 : Reset Statistics ボタンは、 Home ページで報告された統計情報もリセットします。
Display	ディスプレイのポート番号。
Maximum Rate	この列は取り付けられたディスプレイのリフレッシュレートを表します。 Image ページの Maximum Rate フィールドが 0 (つまり、無制限) に設定されている場合は、最大レートがモニタのリフレッシュレートから取得されます。 Image ページの Maximum Rate フィールドが 0 より大きい値に設定されている場合は、リフレッシュレートが "User Defined" として表示されます。
Output Process Rate	ホスト上のイメージエンジンからクライアントに現在送信されているフレームレート。
Image Quality	取り付けられたディスプレイの現在のロスレス状態を示します。 <ul style="list-style-type: none"> • Lossy • Perceptually lossless • Lossless

5.28.7 OSD : セッション統計情報設定

Session Statistics ページでは、最後のセッションの統計方法を表示することができます。このページは、**Options > Diagnostics > Session Statistics** メニューから表示することができます。

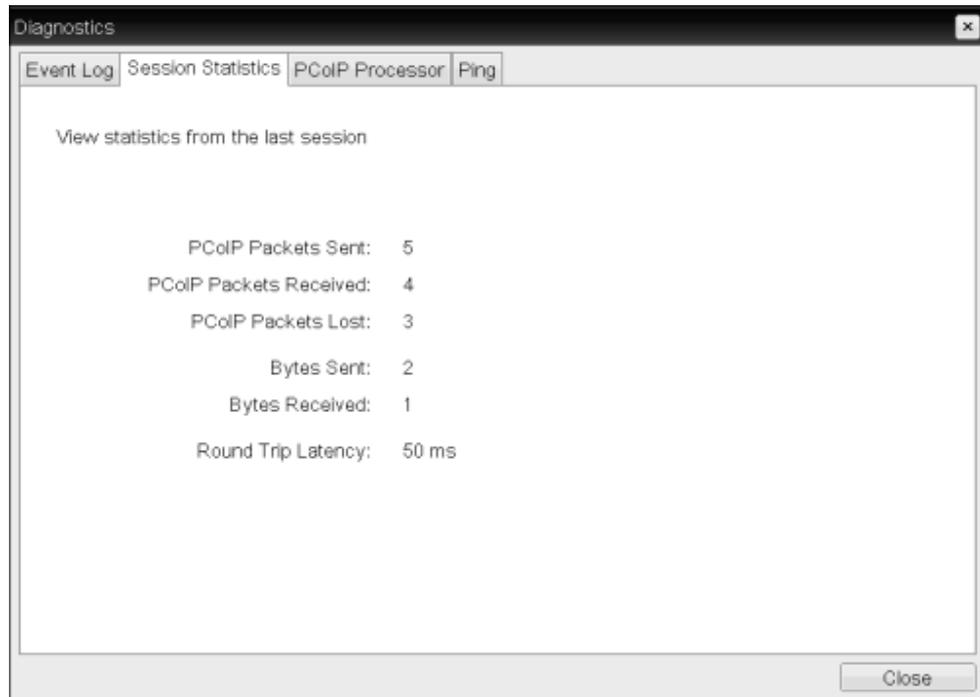


図 5-114 : OSD Session Statistics ページ

表 5-103 : OSD Session Statistics ページパラメータ

パラメータ	説明
PCoIP Packets Statistics	<p>PCoIP Packets Sent : 最後のセッションで送信された PCoIP パケットの総数。</p> <p>PCoIP Packets Received : 最後のセッションで受信された PCoIP パケットの総数。</p> <p>PCoIP Packets Lost : 最後のセッションで消失された PCoIP パケットの総数。</p>
Bytes	<p>Bytes Sent : 最後のセッションで送信されたバイトの総数。</p> <p>Bytes Received : 最後のセッションで受信されたバイトの総数。</p>
Round Trip Latency	PCoIP システムとネットワークの往復遅延の最小値、平均値、および最大値 (ミリ秒 (+/- 1 ms) 単位)

5.28.8 AWI ホスト : ホスト CPU 設定

Host CPU ページでは、ホストコンピュータの識別文字列を表示したり、現在の電源状態を確認したり、ホストの電源状態を変更したりすることができます。このページは、**Diagnostics > Host CPU** メニューからアクセスすることができます。

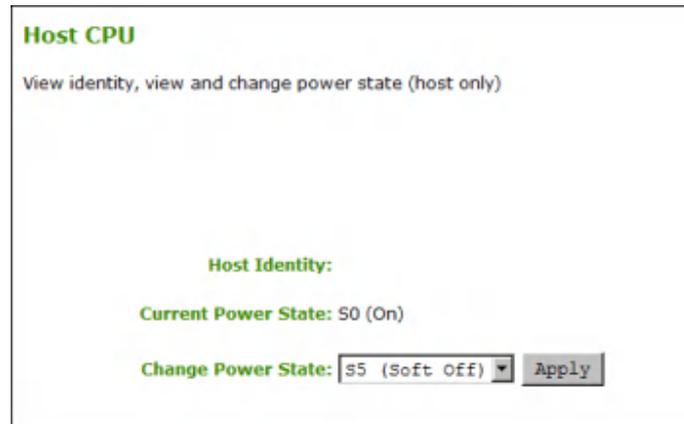


図 5-115 : AWI Host CPU ページ

表 5-104 : AWI Host CPU ページパラメータ

パラメータ	説明
Host Identity	ホストコンピュータの識別文字列（データが入手可能な場合）。
Current Power State	ホストに設定されている現在の電源状態。
Change Power State	<p>以下のオプションの中から選択します。</p> <ul style="list-style-type: none"> • S5 (Soft Off) : 押下時間が 4 秒未満の場合にホストのソフト電源オフを実行する（つまり、ホストをスリープモードにする）ようにクライアントのリモート PC ボタンを設定します。 • S5 (Hard Off) : 押下時間が 4 秒以上の場合にホストのハード電源オフ（つまり、デバイスシャットダウン）を実行するようにクライアントのリモート PC ボタンを設定します。 <p>注意：この機能を使用するには、ホストのハードウェアアーキテクチャに互換性がある必要があります。</p>

5.28.9 AWI クライアント：オーディオ設定

Audio ページでは、クライアントからオーディオテストトーンを再生することができます。このページは、**Diagnostics > Audio** メニューからアクセスすることができます。

オーディオテストトーンを再生するには、**Start** をクリックしてテストトーンを開始します。テストを終了するには、**Stop** をクリックします。

注意： **Audio** ページの機能は、クライアントが PCoIP セッション中でない場合にのみクライアント上で使用することができます。



図 5-116 : AWI クライアント Audio ページ

5.28.10 AWI クライアント : ディスプレイ設定

Display ページでは、クライアントのディスプレイ上でテストパターンを表示して確認することができます。このページは、**Diagnostics > Display** メニューからアクセスすることができます。

注意：テストパターンは、クライアントが PCoIP セッション中でない場合にのみ **Display** ページに表示されます。クライアントがセッション中に **Start** をクリックすると、エラーメッセージが表示されます。

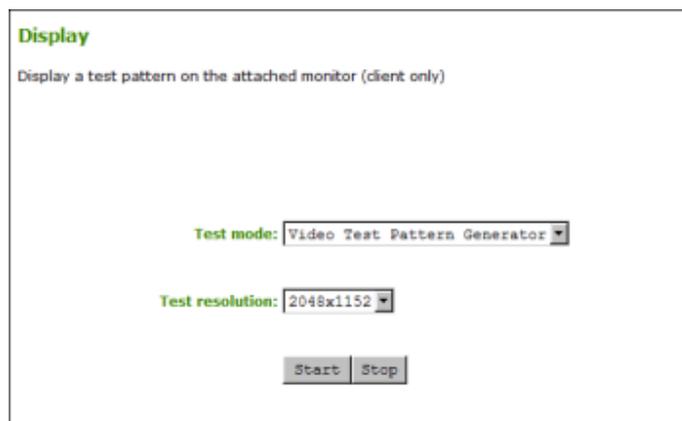


図 5-117 : AWI クライアント Display ページ

表 5-105 : AWI クライアント Display ページパラメータ

パラメータ	説明
Test mode	接続されたモニタのテストパターンのタイプを次のように設定します。 <ul style="list-style-type: none"> • Video Test Pattern Generator • Pseudo Random Bitstream
Test resolution	ドロップダウンメニューから使用するテスト解像度を選択します。
Start/Stop	Start をクリックするとテストパターンが開始されます。テストを終

パラメータ	説明
	了するには、 Stop をクリックします。

5.28.11 AWI : PCoIP プロセッサ設定

PCoIP Processor ページでは、ホストまたはクライアントをリセットしたり、デバイスの PCoIP プロセッサに関する最後のブート以降のアップタイムを表示したりすることができます。このページは、**Diagnostics > PCoIP Processor** メニューからアクセスすることができます。

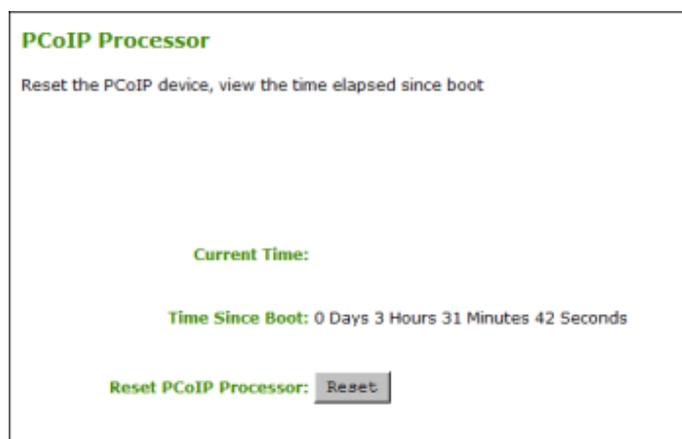


図 5-118 : AWI PCoIP Processor ページ

表 5-106 : AWI PCoIP Processor ページパラメータ

統計情報	説明
Current Time	現在時刻。この機能では、 NTP を有効にして設定する 必要があります。
Time Since Boot (Uptime)	デバイスの PCoIP プロセッサに関する最後のブート以降のアップタイムが表示されます。
Reset PCoIP Processor	このボタンをクリックするとデバイスがリセットされます。

5.28.12 OSD : PCoIP プロセッサ設定

PCoIP Processor ページでは、デバイスの PCoIP プロセッサに関する最後のブート以降のアップタイムを表示することができます。このページは、**Options > Diagnostics > PCoIP Processor** メニューからアクセスすることができます。

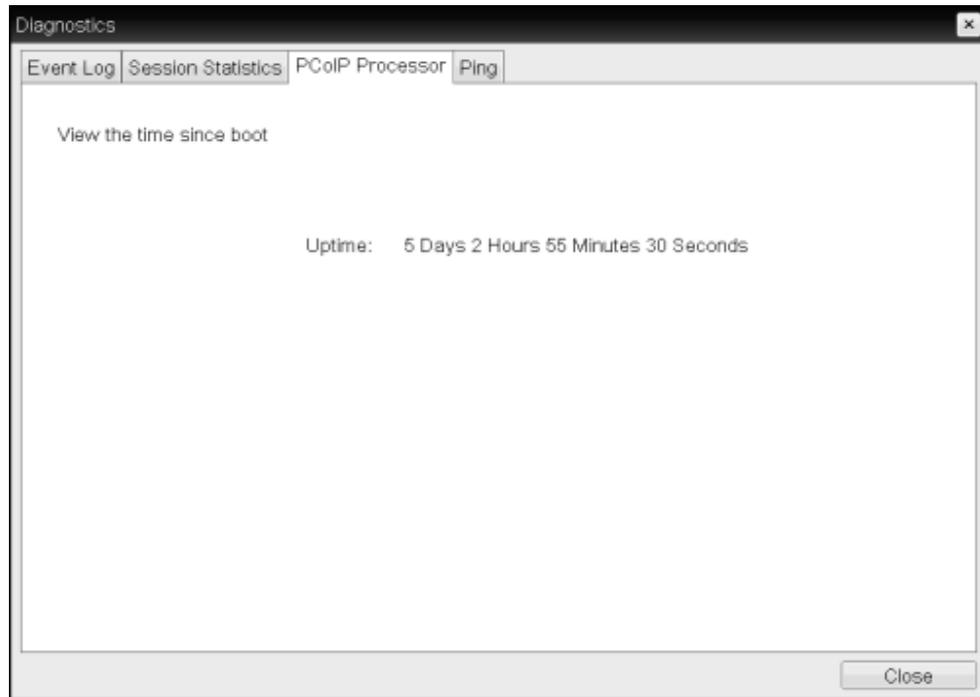


図 5-119 : OSD PCoIP Processor ページ

5.28.13 OSD : Ping 設定

Ping ページでは、デバイスを ping して IP ネットワーク全体に到達可能かどうかを確認することができます。これは、ホストが到達可能かどうかを判断するのに役立つ場合があります。ファームウェアリリース 3.2.0 以降では ping コマンドで「フラグメント不許可フラグ」が強制されるため、この機能を使用して最大 MTU サイズを特定することもできます。

このページは、**Options > Diagnostics > Ping** メニューからアクセスすることができます。

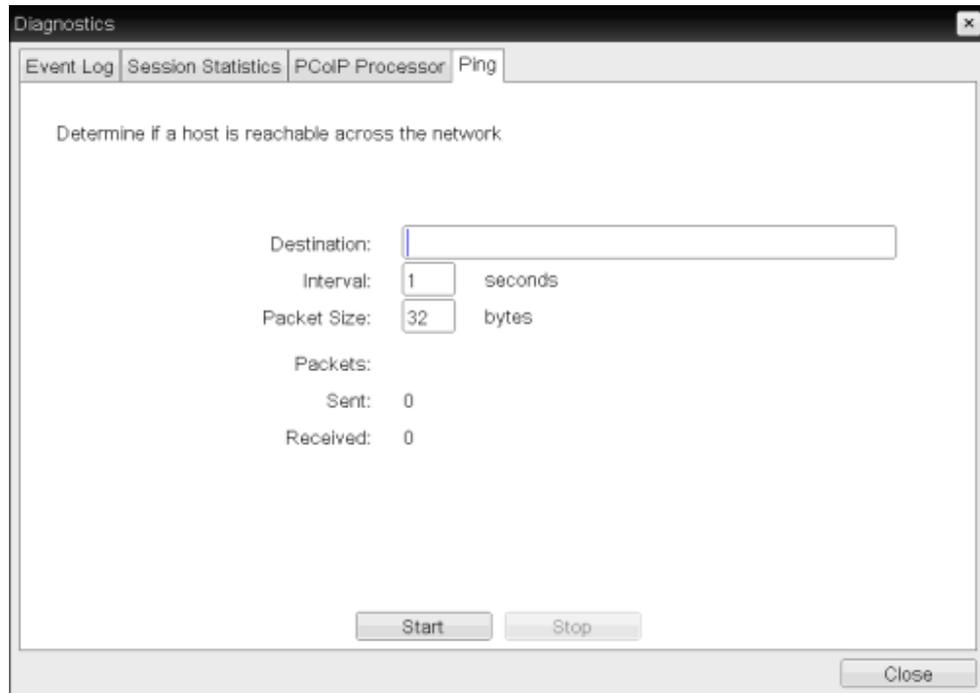


図 5-120 : OSD Ping ページ

表 5-107 : Ping ページパラメータ

パラメータ	説明
Destination	ping する IP アドレスまたは完全修飾ドメイン名 (FQDN)。
Interval	ping パケット間の時間間隔。
Packet Size	ping パケットのサイズ。
Packets Sent	送信された ping パケットの数。
Packets Received	受信された ping パケットの数。

5.29 情報の表示 (AWI/OSD)

5.29.1 AWI : バージョン情報

Version ページでは、デバイスのハードウェアバージョンとファームウェアバージョンの詳細を表示することができます。このページは、**Info > Version** メニューからアクセスすることができます。

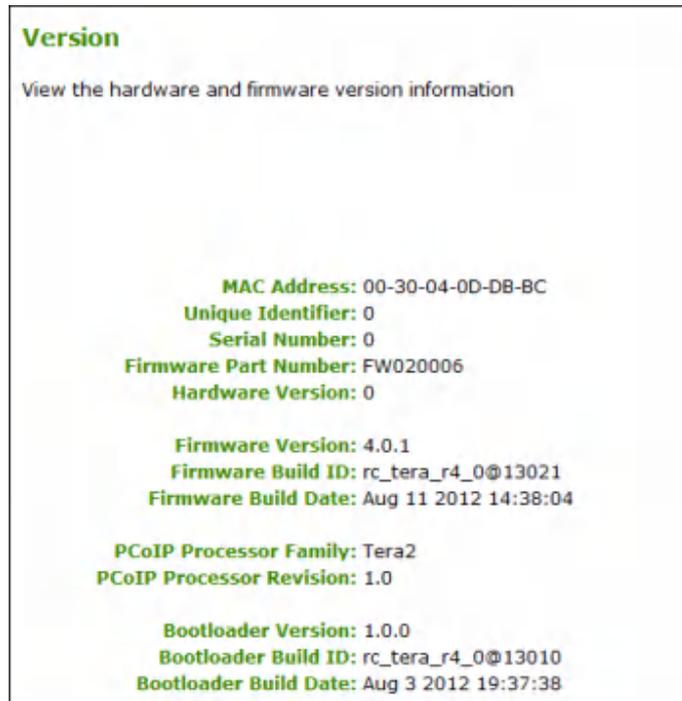


図 5-121 : AWI Version ページ

表 5-108 : AWI Version ページパラメータ

パラメータ	説明
VPD Information	<p>(Vital Product Data) : ホストまたはクライアントを一意に識別するために工場でのプロビジョンされた情報 :</p> <ul style="list-style-type: none"> • MAC Address : ホスト/クライアントの一意の MAC アドレス。 • Unique Identifier : ホスト/クライアントの一意の識別子。 • Serial Number : ホスト/クライアントの一意のシリアル番号。 • Firmware Part Number : 現在のファームウェアの部品番号。 • Hardware Version : ホスト/クライアントハードウェアのバージョン番号。
Firmware Information	<p>この情報には現在のファームウェアの詳細が反映されます。</p> <ul style="list-style-type: none"> • Firmware Version : 現在のファームウェアのバージョン。 • Firmware Build ID : 現在のファームウェアのリビジョンコード。 • Firmware Build Date : 現在のファームウェアのビルド日付。
PCoIP Processor Information	<p>この情報は PCoIP プロセッサに関する詳細を提供します。</p> <ul style="list-style-type: none"> • PCoIP Processor Family : プロセッサファミリ - Tera1 または Tera2。 • PCoIP Processor Revision : PCoIP プロセッサのシリコンリビ

パラメータ	説明
	ジョン。シリコンのリビジョン B は 1.0 として表記されます。
Bootloader Information	この情報には現在のファームウェアブートローダの詳細が反映されま ず。 <ul style="list-style-type: none"> • Bootloader Version : 現在のブートローダのバージョン。 • Bootloader Build ID : 現在のブートローダのリビジョンコード。 • Bootloader Build Date : 現在のブートローダのビルド日付。

5.29.2 バージョン情報の表示

Version ページでは、デバイスのハードウェアバージョンとファームウェアバージョンの詳細を表示することができます。このページは、**Options > Information > Version** メニューからアクセスすることができます。

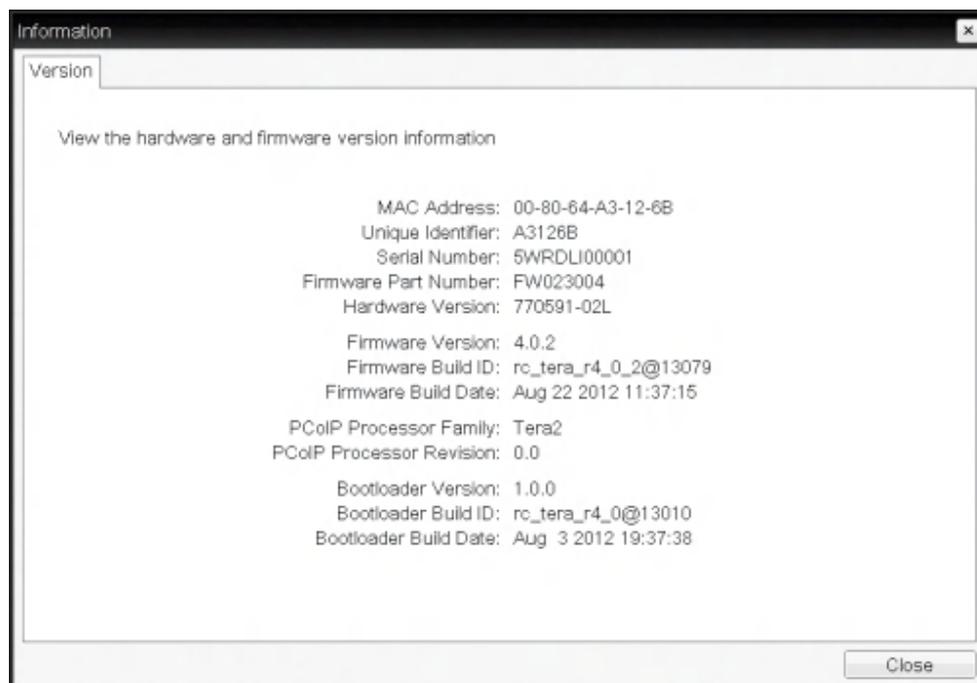


図 5-122 : OSD Version ページ

表 5-109 : OSD Version ページパラメータ

パラメータ	説明
VPD Information	(Vital Product Data) : ホストまたはクライアントを一意に識別するために工場でのプロビジョンされた情報 : <ul style="list-style-type: none"> • MAC Address : ホスト/クライアントの一意の MAC アドレス。 • Unique Identifier : ホスト/クライアントの一意の識別子。

パラメータ	説明
	<ul style="list-style-type: none"> • Serial Number : ホスト/クライアントの一意のシリアル番号。 • Firmware Part Number : 現在のファームウェアの部品番号。 • Hardware Version : ホスト/クライアントハードウェアのバージョン番号。
Firmware Information	<p>この情報には現在のファームウェアの詳細が反映されます。</p> <ul style="list-style-type: none"> • Firmware Version : 現在のファームウェアのバージョン。 • Firmware Build ID : 現在のファームウェアのリビジョンコード。 • Firmware Build Date : 現在のファームウェアのビルド日付。
PCoIP Processor Information	<p>この情報は PCoIP プロセッサに関する詳細を提供します。</p> <ul style="list-style-type: none"> • PCoIP Processor Family : プロセッサファミリー - Tera1 または Tera2。 • PCoIP Processor Revision : PCoIP プロセッサのシリコンリビジョン。シリコンのリビジョン B は 1.0 として表記されます。
Bootloader Information	<p>この情報には現在のファームウェアブートローダの詳細が反映されます。</p> <ul style="list-style-type: none"> • Bootloader Version : 現在のブートローダのバージョン。 • Bootloader Build ID : 現在のブートローダのリビジョンコード。 • Bootloader Build Date : 現在のブートローダのビルド日付。

5.29.3 AWI ホスト : 接続デバイス情報

Attached Devices ページでは、現在クライアントに接続されているディスプレイに関する情報を表示することができます。

Attached Devices								
View presently connected monitors								
Displays:								
Port	Model	Status	Mode	Resolution	Serial	VID	PID	Date
1	BenQ EW2420	Not in Session	DP	1920x1080 @ 60 Hz	V7B00284067	BNQ	7923	30-2011
2	SME2320	Not in Session	DP	No source signal	HVRZA00951	SAM	082	42-2010
3	BenQ EW2420	Not in Session	DP	1920x1080 @ 60 Hz	93B02607026	BNQ	7923	10-2011
4	BenQ BL2400	Not in Session	DP	No source signal	92C00369SL0	BNQ	8002	7-2012

Legend (Displays):	
Status (potential failures)	Description
Connected [EDID read failure / EDID override]	The display is connected and the EDID has been bridged (host/client)
Disconnected	No display or cable has been detected
Not in Session [EDID read failure / EDID override]	The display is connected but we are not in session (client) / we are still asserting hotplug and emulating the following displays (host)
Unknown	On startup on the host, we have not received an EDID request (which determines the mode type) or have not extracted a set of timing (which tells us definitively that we have a cable attached)
Potential Failures	Description
EDID read failure	There was a failure during our DDC channel read of the display EDID. Using a Teradici default EDID.
EDID override	Even though we have not detected a display, we are asserting hotplug and emulating that a Teradici default EDID is attached
Cable error	A dualink conversion cable has been detected on an incorrect port. Dualink conversion cables must be connected to the correct pair of DVI ports. The primary connector (labeled "1") of a conversion cable must be connected to either port 1 or 3 for dualink operation. The secondary connector (labeled "2") on the dualink conversion cable must be plugged into the correct companion port. (ie primary port 1 / secondary port 2; primary port 3 / secondary port 4)

図 5-123 : AWI ホスト Attached Devices ページ

注意：上の図は、4台のディスプレイが接続されたクライアントに関する情報を示しています。デプロイメントで2台のディスプレイが使用されている場合は、2台のディスプレイに関する情報しかこのページに表示されません。

表 5-110 : AWI ホスト : Attached Devices ページ情報

統計情報	説明
Displays	このセクションには、各ポートに接続されたディスプレイのモデル、ステータス、モード、解像度、シリアル番号、ベンダ識別 (VID)、製品識別 (PID)、および日付が表示されます。 注意：このオプションは、ホストが PCoIP セッション中の場合にのみ使用することができます。

5.29.4 AWI クライアント : 接続デバイス情報

Attached Devices ページでは、現在クライアントに接続されているディスプレイに関する情報を表示することができます。

Attached Devices											
View presently connected monitors and USB devices											
Displays:											
Port	Model	Status	Mode	Resolution	Serial	VID	PID	Date			
1	BenQ EW2420	Not in Session	DVI	1920x1080 @ 60 Hz	V7B03284067	0B9Q	7923	20-2011			
2		Disconnected									
3	BenQ EW2420	Not in Session	DVI	1920x1080 @ 60 Hz	92B02607026	0B9Q	7923	10-2011			
4		Disconnected									
USB Devices:											
Device	Parent	Controller	Model	Status	Device Class	Sub Class	Protocol	Serial	VID	PID	Internal/External
1F00	Root 3	OHCI	USB Optical Mouse	Not in Session	00	00	00	-	046D	C03A	External
2001	Root 1	OHCI	USB Keyboard	Not in Session	00	00	00	-	046D	C31C	External
Hide Legend											
Legend (Displays):											
Status (potential failures):											
Connected [EDID read failure / EDID override]				Description The display is connected and the EDID has been bridged (host/client)							
Disconnected				No display or cable has been detected							
Not in Session [EDID read failure / EDID override]				The display is connected but we are not in session (client) / we are still asserting hotplug and enumerating the following displays (host)							
Unknown				On startup on the host, we have not received an EDID request (which determines the mode type) or have not extracted a set of timing (which tells us definitively that we have a cable attached)							
Potential Failures											
EDID read failure				Description There was a failure during our DDC channel read of the display EDID. Using a Teradici default EDID.							
EDID override				Even though we have not detected a display, we are asserting hotplug and emulating that a Teradici default EDID is attached.							
Cable error				A dualink conversion cable has been detected on an incorrect port. Dualink conversion cables must be connected to the correct pair of DVI ports. The primary connector (labeled "1") of a conversion cable must be connected to either port 1 or 2 for dualink operation. The secondary connector (labeled "2") on the dualink conversion cable must be plugged into the correct companion port (ie, primary port 1 / secondary port 3; primary port 2 / secondary port 4).							

図 5-124 : AWI クライアント Attached Devices ページ

表 5-111 : AWI クライアント : Attached Devices ページ情報

統計情報	説明
Displays	<p>このセクションには、各ポートに接続されたディスプレイのモデル、ステータス、モード、解像度、シリアル番号、ベンダ識別 (VID)、製品識別 (PID)、および日付が表示されます。</p> <p>注意：このオプションは、ホストが PCoIP セッション中の場合にのみ使用することができます。</p>
USB Devices	<p>このセクションには、クライアントに接続された USB デバイスのポートモード、モデル、ステータス、デバイスクラス、サブクラス、プロトコル、ベンダ識別 (VID)、および製品識別 (PID) が表示されます。</p>
USB Device Status	<p>次のような状態オプションがあります。</p> <ul style="list-style-type: none"> • Not Connected : デバイスが接続されていません。 • Not in Session : デバイスが PCoIP セッション以外で検出されました。 • Not Initialized : デバイスが PCoIP セッション中に検出されましたが、ホストコントローラがデバイスを初期化していません。 • Failed Authorization : デバイスが PCoIP セッション中に検出されましたが、承認されていません (USB の詳細については、「AWI クライアント : USB 承認」を参照してください)。 • Locally Connected : デバイスが検出され、承認されていますが、PCoIP セッション中にローカルに終端されています (ローカ

統計情報	説明
	ルカーソルなど)。 • Connected : デバイスが PCoIP セッション中に検出され、承認されました。

5.30 ユーザ設定の構成 (OSD)

5.30.1 OSD : VMware View 証明書チェック設定

VMware View ページでは、サーバに対するセキュア接続が確認できない場合のクライアントの動作を選択することができます。このページは、**Options > User Settings > VMware View** メニューからアクセスすることができます。

注意 : AWI で **[VCS Certificate Check Mode Lockout](#)** が有効になっている場合は、このページの設定が変更できなくなります。

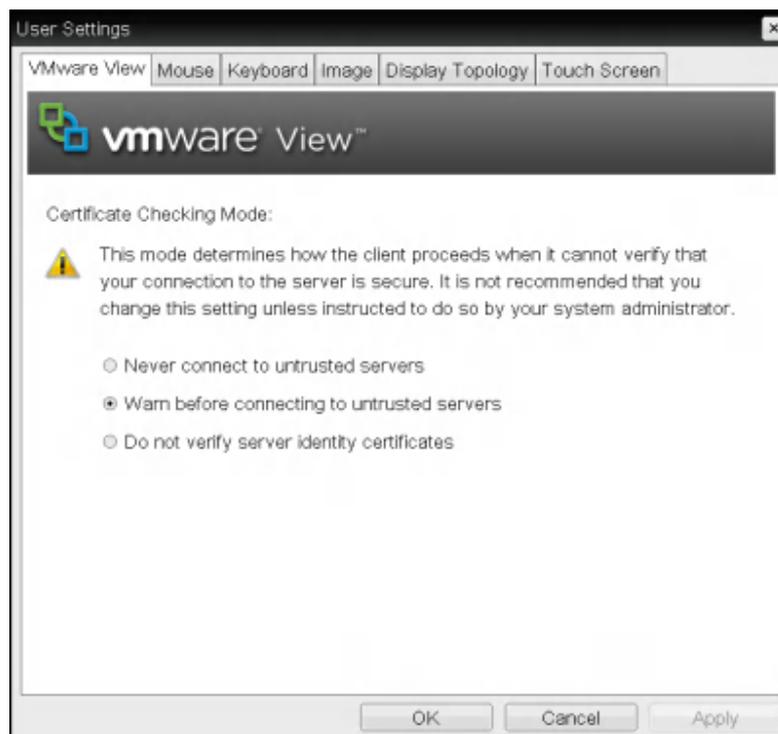


図 5-125 : OSD VMware View ページ

表 5-112 : OSD VMware View ページパラメータ

パラメータ	説明
Never connect to untrusted servers	信頼できる有効な証明書がインストールされていない場合に接続を拒否するようにクライアントを設定します。

パラメータ	説明
Warn before connecting to untrusted servers	未署名のまたは期限切れの証明書を受信した場合、または、証明書が自己署名されておらず、クライアントのトラストストアが空の場合に警告を表示するようにクライアントを設定します。
Do not verify server identity certificates	すべての接続を許可するようにクライアントを設定します。

5.30.2 MC : VMware View 証明書チェック設定に関するヘルプ

管理コンソールに関する証明書チェック設定は、MC の [View Connection Server](#) ページに配置されています。

5.30.3 AWI クライアント : VMware View 証明書チェック設定に関するヘルプ

AWI に関する証明書チェック設定は、AWI クライアントの [View Connection Server](#) ページに配置されています。

5.30.4 OSD : マウス設定

Mouse ページでは、OSD セッションのマウスカーソル速度設定を変更することができます。このページは、**Options > User Settings > Mouse** メニューからアクセスすることができます。

PCoIP ホストソフトウェア経由でもマウスカーソル速度を設定することができます。詳細については、『PCoIP Host Software User Guide』（TER0810001）を参照してください。

注意：PCoIP セッションがアクティブな場合は、**Local Keyboard Host Driver** 機能が使用されていない場合は、OSD マウスカーソル速度設定がマウスカーソル設定に影響を与えることはありません（詳細については、『PCoIP Host Software User Guide』（TER0810001）を参照してください）。この機能は OSD 経由でしか使用することができません。AWI で使用することはできません。

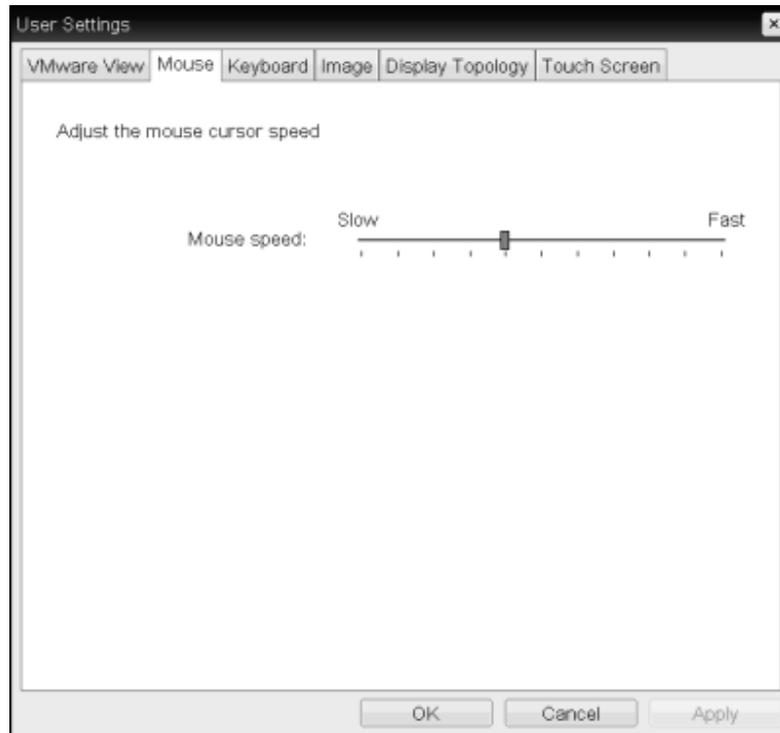


図 5-126 : OSD Mouse ページ

表 5-113 : OSD Mouse ページパラメータ

パラメータ	説明
Mouse Speed	スライダを動かしてマウスカーソルの速度を設定します。

5.30.5 OSD : キーボード設定

Keyboard ページでは、OSDセッションのキーボード文字遅延設定と文字繰り返し設定を変更することができます。このページは、**Options > User Settings > Keyboard** メニューからアクセスすることができます。

PCoIP ホストソフトウェア経由でもキーボード繰り返し設定を構成することができます。詳細については、『PCoIP Host Software User Guide』（TER0810001）を参照してください。

注意 : PCoIPセッションがアクティブな場合は、**Local Keyboard Host Driver** 機能が使用されていないければ、この設定がキーボード設定に影響を与えることはありません（詳細については、『PCoIP Host Software User Guide』（TER0810001）を参照してください）。この機能はOSD経由でしか使用することができません。AWIで使用することはできません。

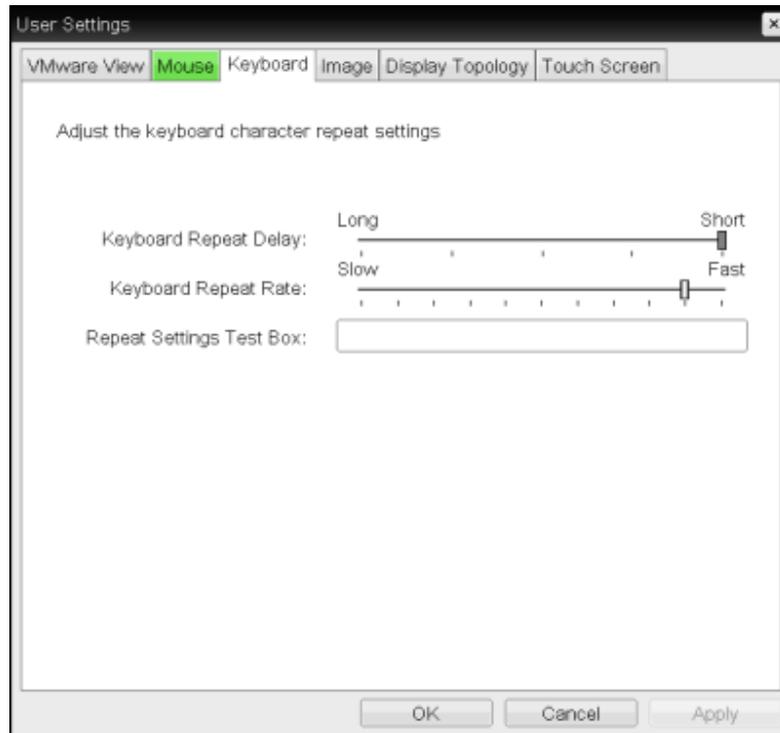


図 5-127 : OSD Keyboard ページ

表 5-114 : OSD Keyboard ページパラメータ

パラメータ	説明
Keyboard Repeat Delay	スライダを動かして、文字を押したままにしたときに繰り返しを開始するまでの時間を設定します。
Keyboard Repeat Rate	スライダを動かして、文字を押したままにしたときに繰り返す速度を設定します。
Repeat Settings Test Box	選択したキーボード設定をテストする場合にこのボックスに入力します。

5.30.6 OSD : イメージ設定に関するヘルプ

OSD の **Image** ページの詳細については、「[OSD : イメージ設定](#)」を参照してください。

5.30.7 OSD : ディスプレイトポロジ設定に関するヘルプ

OSD の **Topology** ページの詳細については、「[OSD : Tera1 ディスプレイトポロジ設定](#)」または「[OSD : Tera2 ディスプレイトポロジ設定](#)」を参照してください。

5.30.8 OSD : タッチスクリーン設定

Touch Screen ページでは、取り付けられた Elo TouchSystems タッチスクリーンディスプレイに関する設定を構成または調整することができます。このページは、**Options > User Settings > Touch Screen** メニューからアクセスすることができます。

注意：**Touch Screen** ページは **OSD 経由でのみ使用することができます**。AWI から使用することはできません。

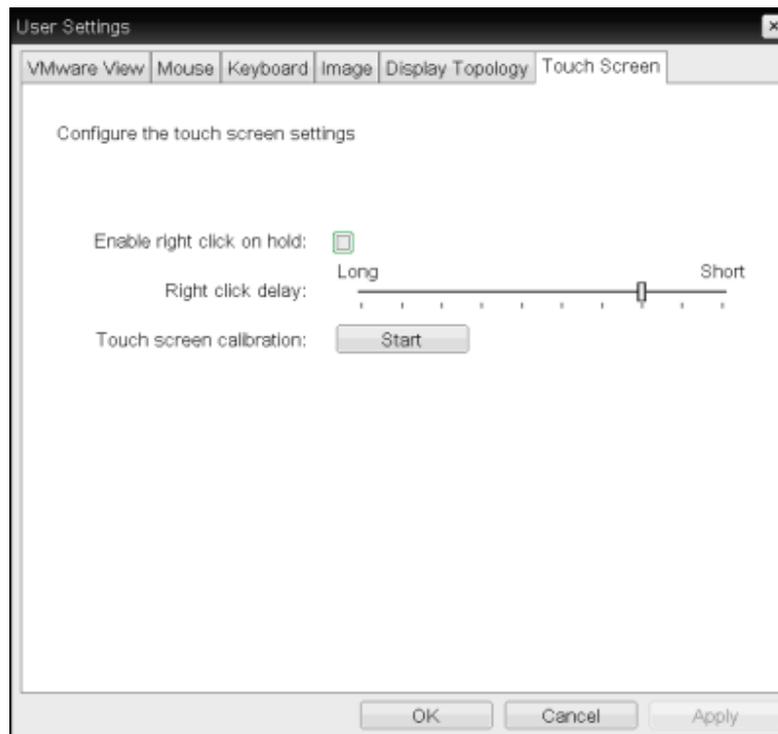


図 5-128 : OSD Touch Screen ページ

表 5-115 : OSD Touch Screen ページパラメータ

パラメータ	説明
Enable right click on hold	このチェックボックスは、ユーザが画面に触れて数秒間そのままにしたときに右クリックを生成できるようにする場合に選択します。無効になっている場合は、右クリック操作がサポートされません。
Right click delay	ユーザが画面に触れたままにして右クリックを生成するまでに必要な時間を決定する位置（Long と Short の間）にポインタをスライドさせます。
Touch screen calibration	初めてタッチスクリーンをゼロクライアントに接続すると、キャリブレーションプログラムが起動します。タッチスクリーンでは、表示された 3 つのターゲットのそれぞれをタッチします。 キャリブレーションをテストするには、指をモニタに沿って移動させ、カーソルが追従することを確認します。成功しなかった場合は、

パラメータ	説明
	キャリブレーションプログラムが自動的に再起動します。キャリブレーションが完了すると、座標がフラッシュに保存されます。 手動でキャリブレーションプログラムを開始するには、 OSD Touch Screen ページで Start をクリックします。オンスクリーンプロンプトに従います。

タッチスクリーンのゼロクライアントへの取り付け

1. タッチスクリーンの USB ケーブルをゼロクライアントの USB ポートに差し込みます。
2. モニタケーブルをタッチスクリーンからゼロクライアントの DVI 1 ポートに取り付けます。

注意：タッチスクリーンの他に非タッチスクリーンモニタをゼロクライアントに取り付けることができます（複数のタッチスクリーンをゼロクライアントに取り付けることはできません）。タッチスクリーンを DVI1 に取り付け、2つ目の非タッチスクリーンモニタを DVI2 に取り付ける必要があります。タッチスクリーンだけをゼロクライアントに取り付ける場合は、DVI1 と DVI2 のどちらにも取り付けることができます。

3. 電源をオンにします。
4. ゼロクライアントセッションを切断します。これにより、タッチスクリーンのキャリブレーションが開始されます。

注意：タッチスクリーンのキャリブレーションが完了したら、座標がフラッシュメモリに保存されます。必要に応じて、**OSD Touch Screen** ページを通して手動でスクリーンのキャリブレーションをやり直すことができます。

5. タッチスクリーンプロンプトに従います。指でキャリブレーションをテストすることができます（カーソルが指と一緒に移動するはずですが）。スクリーンが正しくキャリブレートされていない場合は、システムが自動的にキャリブレーションプログラムを再起動します。

タッチスクリーンのブリッジデバイスとしての設定

注意：この手順は、省略可能で、タッチスクリーンをブリッジデバイスとしてセットアップしたい場合にのみ必要です。

セッションがアクティブの間に、ホスト上で動作しているドライバからタッチスクリーンを制御したい場合があります。これをセットアップするには、タッチスクリーンをブリッジデバイスのリストに追加する必要があります。

1. 以前の手順内のステップに従って、タッチスクリーンをゼロクライアントに取り付けます。
2. ゼロクライアントの管理用ウェブインターフェースにログインします。
3. **Info** メニューで、**Attached Devices** をクリックします。

4. タッチスクリーンの詳細がこのページに表示されるはずですが、**PID** 情報と **VID** 情報を書き留めます。

Attached Devices
View presently connected monitors and USB devices

Displays:								
Port	Model	Status	Mode	Resolution	Serial	VID	PID	Date
1	BenQ EW2420	Connected	DVI	1920x1080 @ 60 Hz	V7B50284067	8BQ	7923	30-2011
2		Disconnected						
3	BenQ EW2420	Connected	DVI	1920x1080 @ 60 Hz	93B02607026	8BQ	7923	10-2011
4		Disconnected						

USB Devices:											
Device	Parent	Controller	Model	Status	Device Class	Sub Class	Protocol	Serial	VID	PID	Internal/External
1F00	Root 3	OHCI	USB Optical Mouse	Locally Connected	00	00	00	-	046D	C05A	External
2901	Root 1	OHCI	USB Keyboard	Locally Connected	00	00	00	-	046D	F11C	External
2102	Root 0	OHCI	Elo TouchSystems 2750 InraTouch USB Touchmonitor Interface	Locally Connected	00	00	00	20626185	04E7	0020	External

5. **Permissions** メニューで、**USB** をクリックして **USB** ページを表示します。
6. **Bridged Devices** エリアで、**Add New** をクリックします。

USB
Configure the USB permissions table

Authorized Devices:

Any Device Class Any Sub Class Any Protocol

Unauthorized Devices: Table is empty

Bridged Devices: Table is empty

Vendor ID:

Product ID:

7. タッチスクリーンのベンダ ID と製品 ID を入力してから、**Apply** をクリックします。
8. ゼロクライアントセッションを再起動します。
9. Elo TouchSystems 製のタッチスクリーンドライバをインストールします。インストールとキャリブレーションの手順については、Elo TouchSystems のマニュアルを参照してください。

ゼロクライアントから VMware View ホストへの自動ログインの設定

タッチスクリーンデバイスへのログインをもっと簡単にするために、**VMware View Login** ウィンドウでキーボードをバイパスするように選択することができます。このセットアップを選択した場合は、**VMware View Login** ウィンドウで **Connect** をタッチする必要があります（または、ユーザ名とパスワードを入力してから、**Connect** をタッチする必要があります）。

1. 管理用ウェブインターフェースにログインします。

2. **Configuration** メニューで、**Session** を選択します。
3. **Session Connection Type** ドロップダウンメニューで、**View Connection Server + Auto-Logon** を選択します。
4. VMware View Connection Server の DNS 名または IP アドレスを入力します。
5. ユーザ資格情報を入力してから、**Apply** をクリックします。

6 PCoIP テクノロジリファレンス

6.1 PCoIP ホストカード

PCoIP ホストカードは、タワーPC、ラックマウント PC、PC ブレード、およびサーバブレードに内蔵することが可能な小型のアドインカードです。このカードの TERA シリーズプロセッサは、ユーザのフルデスクトップ環境をエンコードするための高度な表示圧縮アルゴリズムを実行します。その後で、この情報が IP ネットワーク経由でリアルタイムにユーザの PCoIP ゼロクライアントに送信されます。

PCoIP ホストカードの詳細については、<http://www.teradici.com> にある Teradici ウェブサイトを参照してください。

6.2 PCoIP ゼロクライアント

PCoIP ゼロクライアントは、仮想デスクトップまたはリモートホストワークステーションをローカルまたはワイドエリア IP ネットワーク経由で接続可能にするセキュアなクライアントエンドポイントです。このクライアントは、小型のスタンドアロンデバイス、PCoIP 内蔵ディスプレイ、VoIP 電話機、タッチスクリーンモニタなどのさまざまなフォームファクタを取ることができます。ゼロクライアントは、複数のワイドスクリーンフォーマット、HD オーディオ、およびローカル USB 周辺機器をサポートします。また、近接型カードやスマートカードで使用するための多要素認証を含む、拡張可能な USB セキュリティおよび認証機能を備えています。

シングル TERA シリーズプロセッサで補強されたゼロクライアントは、豊富なマルチメディア体験をユーザに提供します。ユーザは、あらゆる種類のゼロクライアントからデスクトップを操作することも、ゼロクライアントデバイス間を移動しながら同じセッションを維持することもできます。

PCoIP ゼロクライアントの詳細については、<http://www.teradici.com> にある Teradici ウェブサイトを参照してください。

6.3 DVI インターフェースと DisplayPort インターフェース

Tera2 ゼロクライアントは、DVI デジタルディスプレイインターフェースと DisplayPort デジタルディスプレイインターフェースの両方をサポートします。次のようなポートオプションを使用することができます。

- TERA2321 DVI-I デュアルディスプレイ PCoIP ゼロクライアント：2つの DVI ポートがあります。
- TERA2321 DP+DVI-I デュアルディスプレイ PCoIP ゼロクライアント：1つの DVI ポートと 1つの DisplayPort ポートがあります。

- TERA2140 DVI-D クアッドディスプレイ PCoIP ゼロクライアント：4つの DVI ポートがあります。
- TERA2140 DP クアッドディスプレイ PCoIP ゼロクライアント：4つの DisplayPort ポートがあります。

6.3.1 2560x1600 ディスプレイ解像度のサポート

上記ゼロクライアントのすべてが、DVI インターフェースまたは DisplayPort インターフェースを備えた付属モニタの 2560x1600 解像度もサポートします。ただし、DVI インターフェースでこの解像度をサポートするには、カスタムデュアルリンク DVI ケーブルアダプタが必要です。

下の図は、ビデオケーブルと各種ゼロクライアントを接続して接続先のディスプレイで 2560x1600 解像度を実現する方法を示しています。

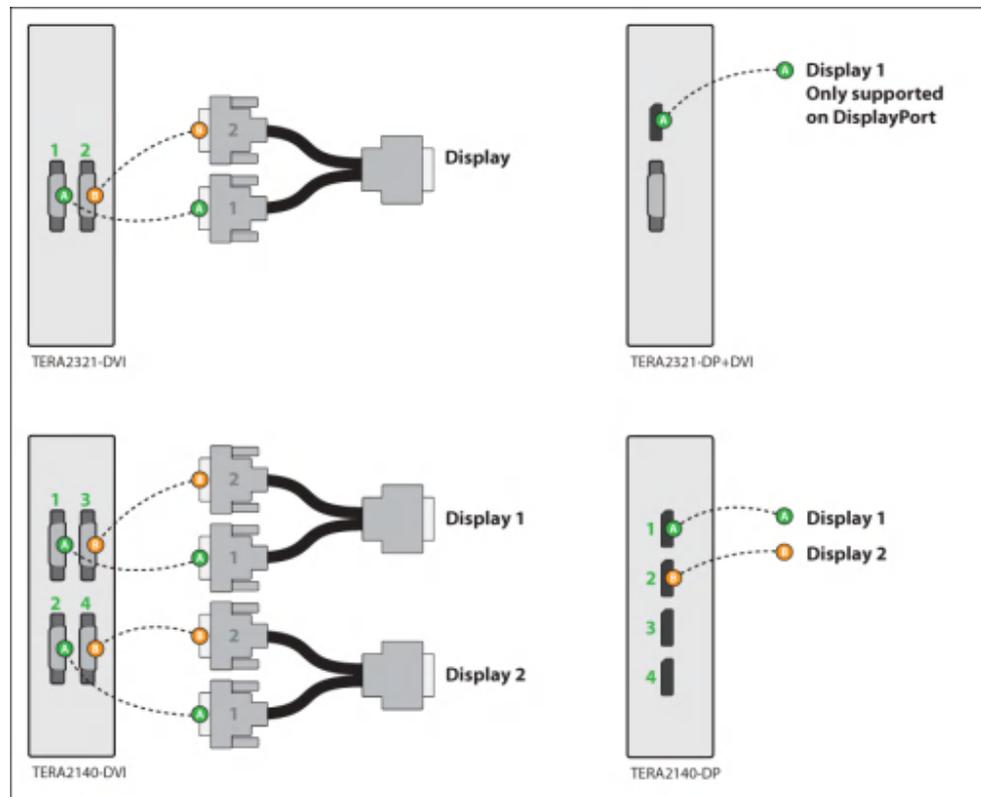


図 6-1 : 2560x1600 解像度用の DVI コネクタと DisplayPort コネクタ

- TERA2321 DVI-I デュアルディスプレイ PCoIP ゼロクライアント：このゼロクライアントは 1つの 2560x1600 モニタをサポートします。上の図（左上）に示すように、カスタムデュアルリンク DVI-I ケーブルアダプタの 2つの DVI-I ケーブルコネクタをゼロクライアントの 2つの DVI-I ポートに接続します。
- TERA2321 DP+DVI-I デュアルディスプレイ PCoIP ゼロクライアント：このゼロクライアントは DisplayPort インターフェースを介して 1つの 2560x1600 モニタの

みをサポートします。上の図（右上）に示すように、DisplayPort ケーブルのコネクタをゼロクライアントの DisplayPort ポートに接続します。

- TERA2140 DVI-D クアッドディスプレイ PCoIP ゼロクライアント：このクライアントは最大 2 つの 2560x1600 解像度モニタをサポートします。上の図（左下）に示すように、モニタごとに、カスタムデュアルリンク DVI-D ケーブルアダプタの 2 つの DVI-D ケーブルコネクタを 2 つの DVI-D ポートに接続します。これらのコネクタは図と全く同様にクライアントのポートに接続する必要があります。
- TERA2140 DP クアッドディスプレイ PCoIP ゼロクライアント：このゼロクライアントは最大 2 つの 2560x1600 モニタをサポートします。上の図（右下）に示すように、DisplayPort ケーブルのコネクタをゼロクライアントの DisplayPort ポートに接続します。

注意：その他の解像度オプションの詳細については、「[PCoIP ホストカードとゼロクライアント](#)」を参照してください。

6.4 PCoIP コネクションブローカ

PCoIP コネクションブローカは、ゼロクライアントから接続を確立しているユーザの ID に基づいて動的にホスト PC をゼロクライアントに割り当てるリソースマネージャです。コネクションブローカはホストのプールをゼロクライアントのグループに割り当てるためにも使用されます。PCoIP デプロイメント内のゼロクライアントが常に同じホストに接続するように設定されている（つまり、静的 1 対 1 ペアリング）場合は、コネクションブローカが必要ありません。

ゼロクライアントとホスト PC を接続するために、複数のサードパーティ製コネクションブローカが PCoIP テクノロジをサポートしています。詳細については、[Teradici サポートサイト](#)で知識ベースサポートトピック 15134-24 を参照してください。

VDI 実装では、ゼロクライアントを VMware View 仮想デスクトップに接続するために VMware View コネクションブローカが使用されます。VMware View コネクションブローカを使用して、PCoIP クライアントとホスト PC を接続することもできます。詳細については、『Using PCoIP Host Cards with VMware View』（TER0911004）を参照してください。

6.5 APEX 2800 PCoIP サーバオフロードカード

APEX 2800 PCoIP サーバオフロードカードは、仮想デスクトップインフラストラクチャ（VDI）実装にハードウェア駆動型 PCoIP イメージエンコーディングを提供します。このカードは、仮想マシンごとのグラフィックエンコーディング要求を継続的に監視しながら、イメージ圧縮タスクを CPU 内のソフトウェアイメージエンコーディングからハードウェアイメージエンコーディングに切り替えたり、元に戻したりします。このオフローディングは、ユーザが切り替えを通知されることなく、必要に応じて、すばやくシームレスに実行されます。

APEX 2800 PCoIP サーバオフロードカードの詳細については、
<http://www.teradici.com>にある Teradici ウェブサイトを参照してください。

7 用語集（略語、頭字語）

256 ビット Salsa20

Salsa20 は 256 ビットのストリーム暗号暗号化アルゴリズムです。

AC

Alternating Current（交流電流）

AES

Advanced Encryption Standard（高度暗号化標準）

AWI

Administrative Web Interface（管理用ウェブインターフェース）。PCoIP ゼロクライアントとホストカードの監視と設定に使用される PCoIP デバイス。AWI に接続するには、サポートされているブラウザに PCoIP デバイスの IP アドレスを入力するだけです。

BIOS

Basic Input/Output System（基本入出力システム）

CA

Certificate Authorities（認証局）

CAC

Common Access Card（共通アクセスカード）。スマートカードの一種。

CAD

Computer Aided Design（コンピュータ支援設計）

CMI

Connection Management Interface（接続管理インターフェース）。外部接続管理サーバとの通信に使用されるホストまたはクライアントから提供されるインターフェース。

CMS

Connection Management Server（接続管理サーバ）。ホストとクライアントを管理可能な外部のサードパーティ製管理エンティティ。コネクションブローカと呼ばれることもあります。

DA

Directory Agent（ディレクトリエージェント）

DDC

Display Data Channel（ディスプレイデータチャンネル）

DDC/CI

Display Data Channel/Command Interface（ディスプレイデータチャンネル/コマンドインターフェース）

DHCP

Dynamic Host Configuration Protocol（動的ホスト構成プロトコル）

DMS-59

2つの DVI ストリームを1つのコネクタにまとめることができるコンピュータビデオカード上の 59 ピンコネクタ

DNS

Domain Name System (ドメインネームシステム)

DNS-SRV

Domain Name System Service Record (ドメインネームシステムサービスレコード)

DVI

Digital Visual Interface (デジタルビジュアルインターフェース)

EDID

Extended Display Identification Data (拡張ディスプレイ識別データ)

EEPROM

Electrically Erasable Programmable Read-Only Memory (電氣的消去可能 ROM)

ESP

Encapsulating Security Payload (セキュリティペイロード隠蔽)

Fps

Frames per second (1秒あたりのフレーム数)。ディスプレイデータフレーム更新速度。

FQDN

Fully Qualified Domain Name (完全修飾ドメイン名)

GPIO

General Purpose Input/Output (汎用入出力)

GPO

Group Policy Object (グループポリシーオブジェクト)

GPU

Graphics Processing Unit (グラフィックスプロセッシングユニット)

GUI

Graphical User Interface (グラフィカルユーザインターフェース)

HD

High Definition (高解像度)

HDCP

High-bandwidth Digital Content Protection (高帯域幅デジタルコンテンツ保護)

HID

Human Interface Device (ヒューマンインターフェースデバイス)

HomePlug

電力線経由のネットワークテクノロジー

HPDET

Hot Plug Detect (ホットプラグ検出)

HTML

Hyper Text Markup Language (ハイパーテキストマークアップランゲージ)

ID

Identification (識別)

IP

Internet Protocol (インターネットプロトコル)

IPsec

Internet Protocol Security (インターネットプロトコルセキュリティ)

IPsec-ESP

Internet Protocol Security-Encapsulated Security Payload (インターネットプロトコルセキュリティ-セキュリティペイロード隠蔽)

IPv4

Internet Protocol Version 4 (インターネットプロトコルバージョン4)。インターネット上の主要なネットワークレイヤプロトコル。

IPv6

Internet Protocol Version 6 (インターネットプロトコルバージョン6)。IPv4の後継。

LAN

Local Area Network (ローカルエリアネットワーク)

LED

Light-Emitting Diode (発光ダイオード)

MAC

Media Access Control (媒体アクセス制御)。一意のハードウェア識別子。

Mbps

Megabits per second (1秒あたりのメガビット数)

MC

Management Console (管理コンソール)

MIB

Management Information Base (管理情報ベース)。SNMPで使用されます。

MTU

Maximum Transmission Unit (最大転送単位)

NAT

Network Address Translation (ネットワークアドレス変換)

NTP

Network Time Protocol (ネットワークタイムプロトコル)

OHCI

Open Host Controller Interface (オープンホストコントローラインターフェース)

OS

Operating System (オペレーティングシステム)

OSD

On Screen Display (オンスクリーンディスプレイ)。ゼロクライアントに表示されるインターフェース。OSDには、接続ダイアログだけでなく、ユーザと管理者の両方からアクセス可能なローカル設定オプションも表示されます。管理者は、必要に応じて、設定オプションを制限したり、ユーザに表示しないようにしたりすることができます。

PC

Personal Computer (パーソナルコンピュータ)

PCI

Peripheral Component Interconnect (ペリフェラルコンポーネントインターコネクタ)

PCLe

Peripheral Component Interconnect Express (ペリフェラルコンポーネントインターコネクタエクスプレス)

PCoIP

Personal Computer over Internet Protocol (パーソナルコンピュータオーバーインターネットプロトコル)

PCoIP ホスト

PCoIP システムのホスト側

PCoIP ゼロクライアント

PCoIP システムのクライアント (ポータル) 側。PCoIP ポータルと呼ばれることもあります。

PC-over-IP

Personal Computer over Internet Protocol (パーソナルコンピュータオーバーインターネットプロトコル)

POST

Power On Self Test (パワーオンセルフテスト)

RDP

Remote Desktop Protocol (リモートデスクトッププロトコル)

RFC

Request for Comments (リクエストフォーコメント)。インターネット規格文書。

SA

Service Agent (サービスエージェント)

SLAAC

Stateless Address Auto-Configuration (ステートレスアドレス自動設定)

SLP

Service Location Protocol (サービスロケーションプロトコル)

SNMP

Simple Network Management Protocol (簡易ネットワーク管理プロトコル)

SSL

Secure Socket Layer (セキュアソケットレイヤ)。セキュリティプロトコルの1つ。

TERA1100

PCoIP ゼロクライアント機能をサポートする第1世代 Teradici プロセッサ

TERA1200

PCoIP ホスト機能をサポートする第1世代 Teradici プロセッサ

TERA2140

PCoIP ゼロクライアント機能をサポートする第2世代 Teradici プロセッサ

TERA2220

PCoIP ホスト機能をサポートする第2世代 Teradici プロセッサ

TERA2240

PCoIP ホスト機能をサポートする第2世代 Teradici プロセッサ

TERA2321

PCoIP ゼロクライアント機能をサポートする第2世代 Teradici プロセッサ

UA

User Agent (ユーザエージェント)

UDP

User Datagram Protocol (ユーザデータグラムプロトコル)

UI

User Interface (ユーザインターフェース)

USB

Universal Serial Bus (ユニバーサルシリアルバス)

VDI

Virtual Desktop Infrastructure (仮想デスクトップインフラストラクチャ)

VGA

Video Graphics Array (ビデオグラフィックスアレイ)

VM

Virtual Machine (仮想マシン)

VPD

Vital Product Data (重要プロダクトデータ)。ホストまたはクライアントを一意に識別するために工場でのプロビジョンされる情報。

VPD (同音異句)

Virtual Desktop Platform (仮想デスクトッププラットフォーム)

VPN

Virtual Private Network (仮想プライベートネットワーク)

WAN

Wide Area Network (広域ネットワーク)。拡張された企業向けの大規模のネットワーク。

WI-FI

IEEE 802.11 無線技術の商標名

WOL

Wake-on-LAN (ウェイクオン LAN)

WOU

Wake-on-USB (ウェイクオン USB)