Unified Contact Center Enterprise (UCCE) Single Sign On (SSO)-Zertifikate und -Konfiguration

Inhalt

Einführung Anforderungen Verwendete Komponenten Teil A. SSO-Nachrichtenfluss Teil B. Zertifikate für IDP und IDS Teil C. IDP-Zertifizierung im Detail und Konfiguration SSL-Zertifikat (SSO) Schritte zum Konfigurieren des SSL-Zertifikats für SSO (lokales Labor mit signierter interner Zertifizierungsstelle) Token-Signaturzertifikat Wie erhält der Cisco IDS-Server den öffentlichen Schlüssel des Token Singing-Zertifikats? Verschlüsselung NICHT aktiviert Teil D. Cisco IDS Side Certificate SAML-Zertifikat

Einführung

Dieses Dokument beschreibt Zertifikatskonfigurationen, die für UCCE SSO erforderlich sind. Die Konfiguration dieser Funktion umfasst mehrere Zertifikate für HTTPS, digitale Signatur und Verschlüsselung.

Anforderungen

Cisco empfiehlt, über Kenntnisse in folgenden Bereichen zu verfügen:

- UCCE-Version 11.5
- Microsoft Active Directory (AD) AD installiert auf Windows Server
- Active Directory Federation Service (ADFS) Version 2.0/3.0

Verwendete Komponenten

UCCE 11,5

Windows 2012 R2

Teil A. SSO-Nachrichtenfluss



Wenn SSO aktiviert ist, meldet sich der Agent bei Finesse Desktop an:

- Finesse-Server leitet Agent-Browser um, um mit Identity Service (IDS) zu kommunizieren
- IDS leitet Agent-Browser mit SAML-Anforderung an Identitätsanbieter (IDP) weiter
- IDP generiert SAML-Token und wird an den IDS-Server weitergeleitet.
- Wenn Token generiert wurde, verwendet der Agent bei jedem Durchsuchen der Anwendung dieses gültige Token für die Anmeldung.

Teil B. Zertifikate für IDP und IDS



IDP-Zertifikate

- SSL-Zertifikat (SSO)
- Token-Signaturzertifikat
- Token Entschlüsseln

| File Action View Window Help | | | | | | |
|------------------------------|---|-------------------------|----------------|-----------------|--------|---------|
| AD FS | Certificates | | | | | |
| Service Fndpoints | Subject | Issuer | Effective Date | Expiration Date | Status | Primary |
| Certificates | Service communications CN=col115dc.col115.org.au, OU=TAC, O=Cisco | CN=col115-COL115-CA, | 12/30/2016 | 12/30/2017 | | |
| | Token-decrypting CN=ADFS Encryption - col115dc.col115.org.au | CN=ADFS Encryption - co | 12/30/2016 | 12/30/2017 | | Primary |
| | Token-signing CN=ADFS Signing - col115dc.col115.org.au | CN=ADFS Signing - col11 | 12/30/2016 | 12/30/2017 | | Primary |

IDS-Zertifikate

- SAML-Zertifikat
- Signaturschlüssel
- Verschlüsselungsschlüssel



Teil C. IDP-Zertifizierung im Detail und Konfiguration

SSL-Zertifikat (SSO)

- Dieses Zertifikat wird zwischen IDP und Client verwendet. Kunde muss SSO-Zertifikat vertrauen
- Das SSL-Zertifikat wird zur Verschlüsselung der Sitzung zwischen dem Client und dem IDP-Server bereitgestellt. Dieses Zertifikat ist nicht für ADFS spezifisch, sondern für IIS.
- Der Betreff des SSL-Zertifikats muss mit dem in der ADFS-Konfiguration verwendeten Namen übereinstimmen.



Schritte zum Konfigurieren des SSL-Zertifikats für SSO (lokales Labor mit signierter interner Zertifizierungsstelle)

Schritt 1: Erstellen Sie ein SSL-Zertifikat mit Zertifikatsanforderung (Certificate Signing Request, CSR), und signieren Sie das Zertifikat von einer internen Zertifizierungsstelle für ADFS.

- 1. Öffnen Sie Server Manager.
- 2. Klicken Sie auf Extras.
- 3. Klicken Sie auf Internetinformationsdienste-Manager (IIS).
- 4. Wählen Sie den lokalen Server aus.
- 5. Wählen Sie Serverzertifikate aus.
- 6. Klicken Sie auf Funktion öffnen (Aktionsbereich).
- 7. Klicken Sie auf Zertifikatsanforderung erstellen.
- 8. Lassen Sie den Kryptografiedienstanbieter standardmäßig unverändert.
- 9. Ändern Sie die Bit-Länge in 2048.
- 10. Klicken Sie auf Weiter.
- 11. Wählen Sie einen Speicherort für die angeforderte Datei aus.
- 12. Klicken Sie auf Fertig stellen.

| Server Mana | ager | | | | | | | - | o > |
|----------------------------------|-----------------------|----------------|------|---|--|---|---|-------|------------|
| | | | • (; | ि। | ľ., | Manage | Tools | View | Help |
| | | | | Active Active Active | Director Director | y Administr y Domains a y Module fo | ative Cente and Trusts or Windows | Power | Shell |
| bility | Last Update | Windows Activa | | Active | Director | y Sites and | Services | | |
| Performance counters not started | 1/10/2017 12:59:07 PM | Not activated | | Active AD FS ADSI E Certifi Comp Defrag DNS Event Group | Director Manage Edit cation Au onent Se uter Man gment an Viewer Policy N et Inform | y Users and ment uthority rvices agement of Optimize | Drives | Manao | er |
| | | | | Intern | et Inform | ation Service | ces (IIS) Mar | nager | |

| \$ 3 | Internet Information Services (IIS) Manager | _ 🗆 X |
|--------------------------------|---|--------------------------|
| 0 | Sol → FS01 → | 📅 🗟 🏠 🔞 - |
| File View | Request Certificate ? | × |
| • 2 Start | Cryptographic Service Provider Properties | Request |
| () A ⊳- ⊗ Si | Select a cryptographic service provider and a bit length. The bit length of the encryption key determines the certificate's encryption strength. The greater the bit length, the stronger the security. However, a greater bit length may decrease performance. | rtificate Certificate |
| | Cryptographic service provider: | |
| | Bit length: | |
| | 2048 🗸 | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | Previous Next Finish Cancel | |
| | | |
| < | III Features View Content View | |
| Ready | | • <u>1</u> .: |

Schritt 2: CA signiert die aus Schritt 1 generierte CSR-Anfrage.

- 1. Öffnen Sie den CA-Server, um diesen CSR http:<CA-Server-IP-Adresse>/certsrv/zu verwenden.
- 2. Klicken Sie auf Zertifikat anfordern.
- 3. Klicken Sie auf Erweiterte Zertifikatsanforderung.
- 4. Kopieren Sie den CSR in eine Base-64-codierte Zertifikatsanforderung.
- 5. Senden.
- 6. Laden Sie das signierte Zertifikat herunter.

Microsoft Active Directory Certificate Services - col115-COL115-CA

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you can verify your ide communicate with over the Web, sign and encrypt messages, and, depending upon the type of certificate you request, perform other security

You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocation list (CRL), or to v pending request.

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:

Request a certificate View the status of a pending certificate request Download a CA certificate, certificate chain, or CRL

Submit a Certificate Request or Renewal Request

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

| Saved Request: | |
|---|----------|
| Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7): | |
| Additional Attributes: | |
| Attributes: | |
| | Submit > |

Schritt 3: Installieren Sie das signierte Zertifikat zurück zum ADFS-Server, und weisen Sie die ADFS-Funktion zu.

1. Installieren Sie das signierte Zertifikat zurück zum ADFS-Server. Dazu öffnen Sie den Server Manager > Extras > Internetinformationsdienste (IIS)-Manager > .

Lokaler Server > Serverzertifikat > Funktion öffnen (Aktionsbereich).

2. Klicken Sie auf Abschlusszertifikatanforderung.

3. Wählen Sie den Pfad zur vollständigen CSR-Datei aus, die Sie vom Zertifikatanbieter des Fremdherstellers abgeschlossen und heruntergeladen haben.

4. Geben Sie den freundlichen Namen für das Zertifikat ein.

- 5. Wählen Sie als Zertifikatsspeicher Personal aus.
- 6. Klicken Sie auf OK.

| 🕤 📲 🕨 COL115 🕨 | Complete Certificate Request ? X |
|---|---|
| View Help ctions | Specify Certificate Authority Response |
| Start Page COL115 (COL1150\Adminis Application Pools Sites | Complete a previously created certificate request by retrieving the file that contains the certificate authority's response. File name containing the certification authority's response: Friendly name: ADFS Select a certificate store for the new certificate: Personal |

7. In dieser Phase wurden alle Zertifikate hinzugefügt. Nun ist die Zuweisung von SSL-Zertifikaten erforderlich.

8. Erweitern Sie den lokalen Server > Sites erweitern > Standardwebsite auswählen > Auf Bindungen (Aktionsbereich) klicken.

- 9. Klicken Sie auf Hinzufügen.
- 10. Ändern Sie den Typ in HTTPS.
- 11. Wählen Sie Ihr Zertifikat aus dem Dropdown-Menü aus.
- 12. Klicken Sie auf OK.

| COL115 | Sites Default Web Site | 6 |
|---|---|--|
| View Help | Site Bindings ? × | |
| ections Start Page COL115 (COL1 Application Sites Colf Default Default Default Default Default Default Default | Add Site Binding Type: IP address: Port: https All Unassigned Host name: Require Server Name Indication | issid ing: lical al C site |
| | SSL certificate: Not selected Select View OK Cancel | Veb 30 () 443 |

Nun wurde das SSL-Zertifikat für den ADFS-Server zugewiesen.

Hinweis: Bei der Installation der ADFS-Funktion muss ein vorheriges SSL-Zertifikat verwendet werden.

Token-Signaturzertifikat

ADFS generiert selbstsigniertes Zertifikat für Token-Signaturzertifikate. Standardmäßig ist sie für ein Jahr gültig.

Das von IDP generierte SAML-Token wird von einem privaten ADFS-Schlüssel (Token Signing Certificate Private Part) signiert. Anschließend überprüft IDS mithilfe des öffentlichen ADFS-Schlüssels. Dieses garantierte signierte Token wird nicht modifiziert.

Das Token Signing Certificate wird immer dann verwendet, wenn ein Benutzer Zugriff auf eine Anwendung von Drittanbietern (Cisco IDS) erhalten muss.

| % | | AD FS | | |
|--|--|---|---|----|
| 翰 File Action View Window Help | | | Certificate | × |
| 🗢 🔿 🙍 📰 🖬 | | | General Details Certification Path | |
| AD FS AD FS Certificates Claim Descriptions Claims Provider Trusts Relying Party Trusts Authentication Policies Per Relying Party Trust | Certificates Subject Service communications CN=col115dc.col115.org.au, OU=TAC, O=Cisco Token-decrypting CN=ADFS Encryption - col115dc.col115.org.au Token-signing CN=ADFS Signing - col115dc.col115.org.au | Issuer CN=col115-COL11 CN=ADFS Encrypt CN=ADFS Signing | General Details Certification Path Image: Certificate Information This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store. Issued to: ADFS Signing - col115dc.col115.org.au Issued by: ADFS Signing - col115dc.col115.org.au Valid from 12/30/2016 Install Certificate Issuer Statemet | nt |
| | < | ш | , or | (|

Wie erhält der Cisco IDS-Server den öffentlichen Schlüssel des Token Singing-Zertifikats?

Dies geschieht durch das Hochladen von ADFS-Metadaten auf den IDS-Server und anschließendes Übergeben des öffentlichen ADFS-Schlüssels an den IDS-Server. Auf diese Weise erhält IDS den öffentlichen Schlüssel des ADFS-Servers.

Sie müssen IDP-Metadaten von ADFS herunterladen. Informationen zum Herunterladen von IDP-Metadaten finden Sie unter https:// <FQDN of ADFS>/federationmetadata/2007-06/federationmetadata.xml.

| 54 | |
|----------|--|
| 85 | |
| 86 | - <keydescriptor use="signing"></keydescriptor> |
| 87 88 | |
| 89 | - <keyinfo xmlns="http://www.w3.org/2000/09/xmldsig#"></keyinfo> |
| 91 | |
| 93 | - <xs09data></xs09data> |
| 94 | <pre><x509certificate>MIIC6DCCAdCgAwIBAgIQFpYJVs99CK9LN50rHdF5nDANBgkqhkiG9w0BAQsFADAwMS4wLAYDVQQDEyVBREZTIFNpZ25pbmcgLSBjb2wxMTVkYy5jb2wxHTUk 4XDTE2MTIzMDAxHDMyOFoXDTE3MTIzMDAxMDMyOFowMDEuMCwGA1UEAxH1QURGUyBTaWduaW5nIC0gY29eMTE1ZGMuY29eMTE1Lm9yZy5hdTCCASIwDQYJKoZIhwcNAQEBBQADggE gEBAKfeys1epEkwWspH4[IB2hGh12+rbhjwS49Js7FXMUPN3HLMBOCBKM18f5FlddqSQD/wlot4+2kkx6poxKjNpzfuUMU7tqqe1kWDBLoSKu2E70UrDHdq6HvW2HXOKN8j+1+1 http://www.bucku.com/subscience/su</x509certificate></pre> |
| | |

Von ADFS-Metadaten



ADFS-Metadaten auf IDS hochladen Token-Entschlüsselung

Dieses Zertifikat wird automatisch vom ADFS-Server (selbstsigniert) generiert. Wenn das Token verschlüsselt werden muss, verwendet ADFS den öffentlichen IDS-Schlüssel, um ihn zu entschlüsseln. Wenn Sie jedoch ADFS-Token-Verschlüsselung sehen, bedeutet dies NICHT, dass das Token verschlüsselt ist.

| P | CRACPTI WITCHAY | n | | | | | | | |
|---|---|--|-------------------------|----------------|-----------------|--------|---------|-------|---------------|
| I | % | | AD FS | | | | | | |
| I | File Action View Window Help | | | | | | | | |
| l | 🕶 🖤 🔟 📧 🖬 🖬 | Certificates | _ | _ | _ | - | _ | Actio | 005 |
| İ | Service Findmoints | Subject | Issuer | Effective Date | Expiration Date | Status | Primary | Cert | tificates |
| I | Certificates | Service communications CN=col115dc.col115.org au. OU=TAC. 0=Clsco | CN=col115-COL115-CA | 12/30/2016 | 12/30/2017 | | | | Add Token- |
| I | Claim Descriptions | Token-decrypting | | | | | | | Add Token- |
| I | Claims Provider Trusts | CN=ADFS Encryption - col115dc.col115.org.au | CN=ADFS Encryption - co | 12/30/2016 | 12/30/2017 | | Primary | | View |
| I | Attribute Stores | CN=ADFS Signing - col115dc.col115.org.au | CN=ADFS Signing - col11 | 12/30/2016 | 12/30/2017 | | Primary | | New Windo |
| I | Authentication Policies Per Relying Party Trust | | | | | | | ٩ | Refresh |
| | | | | | | | | ? | Help |
| I | | | | | | | | CN= | col115dc |
| | | | | | | | | | View Certifie |

Wenn Sie sehen möchten, ob die Tokenverschlüsselung für eine bestimmte Anwendung eines vertrauenden Drittanbieters aktiviert wurde, müssen Sie die Registerkarte Verschlüsselung für eine bestimmte Anwendung eines Drittanbieters überprüfen.

Dieses Bild zeigt, dass die Tokenverschlüsselung NICHT aktiviert wurde.

| • 🔿 🖄 🔝 🚺 | | | |
|--|--|--|-----|
| AD FS | Relying Party Trusts | | |
| Service Endpoints Certificates Claim Descriptions Trust Relationships Claims Provider Trusts Relying Party Trusts Attribute Stores Authentication Policies | Display Name Device Registration col115idspub.col11! | Enabled Type Identifier coll115idspub.coll115.org.au Properties i.org. Organization Endpoints Proxy Endpoints Notes Advanced Monitoring Identifiers Encryption Signature Accepted Claims Specify the encryption certificate for this relying party trust. Encryption certificate: Issuer: Issuer: Subject: Effective date: Expiration date: Image: Construction date: Image: Construction date: Browse View Remove Image: Construction date: Image: Construction date: | .au |

Verschlüsselung NICHT aktiviert

Teil D. Cisco IDS Side Certificate

- SAML-Zertifikat
- Verschlüsselungsschlüssel
- Signaturschlüssel

SAML-Zertifikat

Dieses Zertifikat wird vom IDS-Server (selbstsigniert) generiert. Standardmäßig ist sie für 3 Jahre gültig.

| dentity Ser | vice Management | administ |
|--|--|---|
| Node | S | |
| Nodes * - indicates I | ≥rimary Node | |
| Node | Status | SAML Certificate Expiry |
| col115idsp | ub.col115.org.au 🗙 🔹 In Service | • 12-14-2019 18:58 (930 days left) |
| Settings File Action View Windo AD FS Certificates Claim Descriptions Claims Provider Trusts Relying Party Trusts Attribute Stores Per Relying Party Trusts Per Relying Party Trust | W Coll115idspub.coll115.org.au Properties X Organization Endpoints Proxy Endpoints Notes Advanced Monitoring Identifiers Encryption Signature Accepted Claims Specify the signature verification certificates for requests from this relying party. Subject Issuer Effective Date Expiration Subject Issuer Effective Date Expiration CN=coll115ids CN=coll115idspu 12/14/2016 6:5 12/14/2 Add View Remove | Certificate General Details Certification Path See Certificate Information This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store. Issued to: coll15/dspub.coll15.org.au Issued by: coll15/dspub.coll15.org.au Valid from 12/14/2016 Install Certificate Issuer Statement |

Dieses Zertifikat wird zum Signieren der SAML-Anforderung und zum Senden an IDP (ADFS) verwendet. Dieser öffentliche Schlüssel befindet sich in den IDS-Metadaten und muss in den ADFS-Server importiert werden.

- 1. SAML SP-Metadaten vom IDS-Server herunterladen
- 2. Rufen Sie https://<ids server FQDN>:8553/idsadmin/auf.
- 3. Wählen Sie Einstellungen aus, laden Sie SAML SP-Metadaten herunter, und speichern Sie sie.



<IntityDescriptor entityID="col115idspub.col115.org.au" xmlns="urn:oasis:names:tc:SAML:2.0:metadata">
- <SPSSODescriptor protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol" WantAssertionsSigned="true" AuthnRequestsSigned="true">
- <SPSSODescriptor use="signing">
- <keyDescriptor use="signing">
- <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
- <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
- <ds:KeyInfo xmlns:ds="http://www.w3.org/2000/09/xmldsig#">
- <ds:X509Data>
- <ds:X509Data>
<ds:X509Data>
<ds:X509Certificate>MIIC+TCCAeGgAwIBAgIEWD4KtDANBgkqhkiG9w0BAQUFADAIMSMwIQYDVQQDExpjb2wxMTVpZHNw
dWIuY29sMTE1Lm9yZy5hdTAeFw0xNjEyMTQwNzU4MjVaFw0xOTEyMTQwNzU4MjVaMCUxIzAhBgNV
BAMTGmNvbDExNWlkc3B1YI5jb2wxMTUub3JnLmF1MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIB

| - V | Add Relying Party Trust Wizard |
|---|---|
| Select Data Source | |
| Steps Welcome Select Data Source Configure Multi-factor Authentication Now? Choose Issuance Authorization Rules Ready to Add Trust Finish | Select an option that this wizard will use to obtain data about this relying party: Import data about the relying party published online or on a local network. Use this option to import the necessary data and certificates from a relying party organization that publishes its federation metadata online or on a local network. Federation metadata address (host name or URL): Example: fs.contoso.com or https://www.contoso.com/app Import data about the relying party from a file Use this option to import the necessary data and certificates from a relying party organization that has exported its federation metadata to a file. Ensure that this file is from a trusted source. This wizard will not validate the source of the file. Federation metadata file location: Enter data about the relying party manually Use this option to manually input the necessary data about this relying party organization. |

Import auf ADFS-Server

| ÷ | | AD F | -2 |
|---|--|---|--|
| File Action View Window | col115idspub.col115.or | rg.au Properties 🛛 🗙 | Certificate X |
| AD FS Certificates Claim Descriptions Trust Relationships | Organization Endpoints Proxy End Proxy End Encryption Monitoring Identifiers Encryption Specify the signature verification certificates party. Subject Issuer Subject Issuer Issuer | Doints Notes Advanced Signature Accepted Claims for requests from this relying Effective Date Expiration 12/14/2016 6:5 12/14/2 | General Details Certification Path Image: Certificate Information Image: Certificate Information This CA Root certificate is not trusted. To enable trust, install this certificate in the Trusted Root Certification Authorities store. |
| Claims Provider Hosts Relying Party Trusts Attribute Stores Authentication Policies Per Relying Party Trust | | | Issued to: col115idspub.col115.org.au Issued by: col115idspub.col115.org.au |
| | < III Add View Pr OK | emove | Valid from 12/14/2016 to 12/14/2019 Install Certificate Issuer Statement |

Überprüfen von ADFS-Seite

Wenn IDS das SAML-Zertifikat neu generiert, das zum Signieren der SAML-Anforderung verwendet wird, führt es einen Metadatenaustausch durch.

Verschlüsselungs-/Signaturschlüssel

Die Verschlüsselung ist standardmäßig nicht aktiviert. Wenn die Verschlüsselung aktiviert ist, muss sie in ADFS hochgeladen werden.

| col115idspub.col115.org.au P | roperties | | | | | | |
|--|---|------------|----------------|-----|--|------------|--|
| Organization Endpoints Proxy Endpoints | Notes Advanced | | | | | | |
| Monitoring Identifiers Encryption Signatu | re Accepted Claims | | | | | | |
| Specify the encryption certificate for this relying party trust. | | AD FS | | | | | |
| Encryption certificate: | | | | | | | |
| Issuer: | Select an Encryption Certificate | | | | | | |
| Subject: Effective date: | (a) a dial dial dial dial dial dial dial di | « Wir | ndows + ADFS + | ~ C | Search ADFS | م | |
| Expiration date: | Organize 👻 New fo | older | | | | · 🔟 🔞 | |
| Browse View Remove | 🔶 Favorites | ^ | Name | | Date modified | Туре | |
| | Desktop | | 📔 ar | | 8/23/2013 1:39 AM | File folde | |
| | Downloads | | 🔒 bg | | 8/23/2013 1:39 AM | File folde | |
| | E Recent places | | 📕 cs | | 8/23/2013 1:39 AM | File folde | |
| | | | 🔰 da | | 8/23/2013 1:39 AM | File folde | |
| | 🌉 This PC | ≡ | 鷆 de | | 8/23/2013 1:39 AM | File folde | |
| | 膧 Desktop | | 鷆 el | | 8/23/2013 1:39 AM | File folde | |
| | Documents | | 鷆 en | | 12/30/2016 11:59 | File folde | |
| | 🗼 Downloads | | 퉬 en-US | | 12/30/2016 11:59 | File folde | |
| | 🐌 Music | | 🍌 es | | 8/23/2013 1:39 AM | File folde | |
| ок с | 📔 Pictures | | 鷆 et | | 8/23/2013 1:39 AM | File folde | |
| | 📔 Videos | | 鷆 fi | | 8/23/2013 1:39 AM | File folde | |
| | 🔊 Local Disk (C:) | | 🍌 fr | | 8/23/2013 1:39 AM | File folde | |
| | 🖄 DVD Drive (D:) I | RĽ | | | | > | |
| | | File name: | | | Certificate Files (*.cer;*.sst;*.p7k ∨ | | |
| | | | | | Open | Cancel | |

Referenz:

http://www.cisco.com/c/en/us/td/docs/voice ip comm/cust contact/contact center/icm enterprise/i cm_enterprise_11_5_1/Configuration/Guide/UCCE_BK_U882D859_00_ucce-featuresguide/UCCE_BK_U882D859_00_ucce-features-guide_chapter_0110.pdf