[MS-ASPROV]:
ActiveSync Provisioning Protocol Specification

Intellectual Property Rights Notice for Open Specifications Documentation

- **Technical Documentation.** Microsoft publishes Open Specifications documentation for protocols, file formats, languages, standards as well as overviews of the interaction among each of these technologies.
- **Copyrights.** This documentation is covered by Microsoft copyrights. Regardless of any other terms that are contained in the terms of use for the Microsoft website that hosts this documentation, you may make copies of it in order to develop implementations of the technologies described in the Open Specifications and may distribute portions of it in your implementations using these technologies or your documentation as necessary to properly document the implementation. You may also distribute in your implementation, with or without modification, any schema, IDL's, or code samples that are included in the documentation. This permission also applies to any documents that are referenced in the Open Specifications.
- **No Trade Secrets.** Microsoft does not claim any trade secret rights in this documentation.
- **Patents.** Microsoft has patents that may cover your implementations of the technologies described in the Open Specifications. Neither this notice nor Microsoft's delivery of the documentation grants any licenses under those or any other Microsoft patents. However, a given Open Specification may be covered by Microsoft's Open Specification Promise (available here: http://www.microsoft.com/interop/osp) or the Community Promise (available here: http://www.microsoft.com/interop/cp/default.mspx). If you would prefer a written license, or if the technologies described in the Open Specifications are not covered by the Open Specifications Promise or Community Promise, as applicable, patent licenses are available by contacting iplg@microsoft.com.
- **Trademarks.** The names of companies and products contained in this documentation may be covered by trademarks or similar intellectual property rights. This notice does not grant any licenses under those rights.
- **Fictitious Names.** The example companies, organizations, products, domain names, e-mail addresses, logos, people, places, and events depicted in this documentation are fictitious. No association with any real company, organization, product, domain name, email address, logo, person, place, or event is intended or should be inferred.

Reservation of Rights. All other rights are reserved, and this notice does not grant any rights other than specifically described above, whether by implication, estoppel, or otherwise.

Tools. The Open Specifications do not require the use of Microsoft programming tools or programming environments in order for you to develop an implementation. If you have access to Microsoft programming tools and environments you are free to take advantage of them. Certain Open Specifications are intended for use in conjunction with publicly available standard specifications and network programming art, and assumes that the reader either is familiar with the aforementioned material or has immediate access to it.

Preliminary Documentation. This Open Specification provides documentation for past and current releases and/or for the pre-release (beta) version of this technology. This Open Specification is final documentation for past or current releases as specifically noted in the document, as applicable; it is preliminary documentation for the pre-release (beta) versions. Microsoft will release final documentation in connection with the commercial release of the updated or new version of this technology. As the documentation may change between this preliminary version and the final version of this technology, there are risks in relying on preliminary documentation. To the extent that you incur additional development obligations or any other costs as a result of relying on this preliminary documentation, you do so at your own risk.

Revision Summary

Date	Revision History	Revision Class	Comments
12/03/2008	1.0.0	Major	Initial Release.
03/04/2009	1.0.1	Editorial	Revised and edited technical content.
04/10/2009	2.0.0	Major	Updated technical content and applicable product releases.
07/15/2009	3.0.0	Major	Revised and edited for technical content.
11/04/2009	3.1.0	Minor	Updated the technical content.
02/10/2010	3.1.0	None	Version 3.1.0 Release
05/05/2010	4.0.0	Major	Updated and revised the technical content.

Table of Contents

1 Introduction

The ActiveSync Provisioning protocol specifies an **XML-based** format that Microsoft Exchange servers use to communicate security policy settings to client devices.

1.1 Glossary

The following terms are defined in [MS-OXGLOS]:

attachment
cabinet file
calendar
collection
encrypted S/MIME messages
header
Hypertext Markup Language (HTML)
Hypertext Transfer Protocol (HTTP)
message
permissions
plain text
Short Message Service (SMS)
storage
store
synchronization
Uniform Resource Identifier (URI)
WAP Binary XML (WBXML)
XML
XML namespace
XML schema

The following terms are specific to this document:

policy key: A stored value that represents the state of a policy or setting.

remote wipe: Functionality that is implemented on a client, initiated by policy or a request from a server, that requires the client to delete all data and settings related to the referenced protocol.

MAY, SHOULD, MUST, SHOULD NOT, MUST NOT: These terms (in all caps) are used as described in [RFC2119]. All statements of optional behavior use either MAY, SHOULD, or SHOULD NOT.

1.2 References

1.2.1 Normative References

We conduct frequent surveys of the normative references to assure their continued availability. If you have any issue with finding a normative reference, please contact dochelp@microsoft.com. We will assist you in finding the relevant information. Please check the archive site, http://msdn2.microsoft.com/en-us/library/E4BD6494-06AD-4aed-9823-445E921C9624, as an additional source.

[MS-ASAIRS] Microsoft Corporation, "ActiveSync AirSyncBase Namespace Protocol Specification", December 2008.

[MS-ASCMD] Microsoft Corporation, "ActiveSync Command Reference Protocol Specification", December 2008.

[MS-ASDOC] Microsoft Corporation, "ActiveSync Document Class Protocol Specification", December 2008.

[MS-ASDTYPE] Microsoft Corporation, "ActiveSync Data Types", December 2008.

[MS-ASWBXML] Microsoft Corporation, "ActiveSync WAP Binary XML (WBXML) Protocol Specification", December 2008.

[MS-OXGLOS] Microsoft Corporation, "Exchange Server Protocols Master Glossary", April 2008.

[RFC2119] Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", RFC 2119, BCP 14, March 1997, http://www.ietf.org/rfc/rfc2119.txt

[XMLNS] Bray, T., Hollander, D., Layman, A., Eds., et al., "Namespaces in XML 1.0 (Third Edition)", December 2009, http://www.w3.org/TR/REC-xml-names/

[XMLSCHEMA1] Thompson, H., Beech, D., Maloney, M., and Mendelsohn, N., Eds., "XML Schema Part 1: Structures", W3C Recommendation, May 2001, http://www.w3.org/TR/2001/REC-xmlschema-1-20010502/

1.2.2 Informative References

None.

1.3 Overview

The Provisioning protocol consists of an **XML schema** that defines the elements that are necessary for an ActiveSync device to specify its capabilities and **permissions**.

1.4 Relationship to Other Protocols

The ActiveSync Document Class protocol [MS-ASDOC] specifies the XML format that is used by the **Provision** command, as specified in [MS-ASCMD].

All simple data types in this document conform to the data type definitions specified in [MS-ASDTYPE].

1.5 Prerequisites/Preconditions

None.

1.6 Applicability Statement

None.

1.7 Versioning and Capability Negotiation

None.

1.8 Vendor-Extensible Fields

None.

1.9 Standards Assignments

None.

2 Messages

2.1 Transport

The ActiveSync Provisioning protocol consists of a series of XML elements that are embedded within a request or response that is associated with the **Provision** command, as specified in [MS-ASCMD].

2.2 Message Syntax

The XML markup that constitutes the Request Body or the Response Body is transmitted between client and server by using **WAP Binary XML (WBXML)**. For details, see [MS-ASWBXML].

The following is the XML schema definition for the ActiveSync Provisioning protocol command request.

```
<?xml version="1.0" encoding="utf-8"?>
<xs:schema
        xmlns:tns="Provision:"
        attributeFormDefault="unqualified"
        elementFormDefault="qualified"
        targetNamespace="Provision:"
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:settings="Settings:">

    <xs:import namespace="Settings:"/>

    <xs:element name="Provision">
        <xs:complexType>
            <xs:sequence>
                <xs:element ref="settings:DeviceInformation" minOccurs="0" maxOccurs="1" />
                <xs:element name="Policies" minOccurs="0" maxOccurs="1">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="Policy" minOccurs="1" maxOccurs="1">
                                <xs:complexType>
                                    <xs:sequence>
                                        <xs:element name="PolicyType" type="xs:string"
minOccurs="1" maxOccurs="1" />
                                        <xs:element name="PolicyKey" type="xs:string"
minOccurs="0" maxOccurs="1" />
                                        <xs:element name="Status" type="xs:string"
minOccurs="0" maxOccurs="1" />
                                    </xs:sequence>
                                </xs:complexType>
                            </xs:element>
                        </xs:sequence>
                    </xs:complexType>
                </xs:element>
                <xs:element name="RemoteWipe" minOccurs="0" maxOccurs="1">
                    <xs:complexType>
                        <xs:sequence>
                            <xs:element name="Status" type="xs:string" minOccurs="1"
maxOccurs="1" />
                        </xs:sequence>
                    </xs:complexType>
                </xs:element>
            </xs:sequence>
        </xs:complexType>
```

```
    </xs:element>
</xs:schema>
```

The following is the XML schema definition for the ActiveSync Provisioning protocol command response.

```
<?xml version="1.0" ?>
<xs:schema
    xmlns:tns="Provision:"
    attributeFormDefault="unqualified"
    elementFormDefault="qualified"
    targetNamespace="Provision:"
    xmlns:xs="http://www.w3.org/2001/XMLSchema">

<xs:element name="Provision">
    <xs:complexType>
        <xs:sequence>
            <xs:element name="Status" type="xs:unsignedByte" />
             <xs:element name="Policies">
                 <xs:complexType>
                     <xs:sequence>
                         <xs:element name="Policy">
                             <xs:complexType>
                                 <xs:sequence>
                                     <xs:element name="PolicyType" type="xs:string" />
                                     <xs:element name="Status" type="xs:unsignedByte" />
                                     <xs:element name="PolicyKey" type="xs:string" />
                                     <xs:element name="Data">
                                         <xs:complexType>
                                          <xs:sequence>
                                           <xs:element name="eas-provisioningdoc">
                                            <xs:complexType>
                                             <xs:sequence>
                                              <xs:element name="DevicePasswordEnabled"
type="xs:boolean" />
                                              <xs:element
name="AlphaNumericDevicePasswordRequired" type="xs:boolean" minOccurs="0" />
                                              <xs:element name="PasswordRecoveryEnabled"
type="xs:boolean" minOccurs="0" />
                                              <xs:element name="DeviceEncryptionEnabled"
type="xs:boolean" minOccurs="0" />
                                              <xs:element name="AttachmentsEnabled"
type="xs:boolean" minOccurs="0" />
                                              <xs:element name="MinDevicePasswordLength"
type="xs:unsignedByte" minOccurs="0" />
                                              <xs:element
name="MaxInactivityTimeDeviceLock" type="xs:unsignedInt" minOccurs="0" />
                                              <xs:element
name="MaxDevicePasswordFailedAttempts" type="xs:unsignedByte" minOccurs="0" />
                                              <xs:element name="MaxAttachmentSize"
type="xs:unsignedInt" minOccurs="0" />
                                              <xs:element
name="AllowSimpleDevicePassword" type="xs:boolean" minOccurs="0" />
                                              <xs:element
name="DevicePasswordExpiration" type="xs:unsignedInt" minOccurs="0" />
                                              <xs:element name="DevicePasswordHistory"
type="xs:unsignedint" minOccurs="0"/>
                                              <xs:element name="AllowStorageCard"
type="xs:boolean" minOccurs="0" />
```

```
                                                <xs:element name="AllowCamera"
type="xs:boolean" minOccurs="0" />
                                                <xs:element name="RequireDeviceEncryption"
type="xs:boolean" minOccurs="0" />
                                                <xs:element
name="AllowUnsignedApplications" type="xs:boolean" minOccurs="0" />
                                                <xs:element
name="AllowUnsignedInstallationPackages" type="xs:boolean" minOccurs="0" />
                                                <xs:element
name="MinDevicePasswordComplexCharacters" type="xs:unsignedByte" minOccurs="0" />
                                                <xs:element name="AllowWiFi"
type="xs:boolean" minOccurs="0" />
                                                <xs:element name="AllowTextMessaging"
type="xs:boolean" minOccurs="0" />
                                                <xs:element name="AllowPOPIMAPEmail"
type="xs:boolean" minOccurs="0" />
                                                <xs:element name="AllowBluetooth"
type="xs:unsignedByte" minOccurs="0" />
                                                <xs:element name="AllowIrDA"
type="xs:boolean" minOccurs="0" />
                                                <xs:element
name="RequireManualSyncWhenRoaming" type="xs:boolean" minOccurs="0" />
                                                <xs:element name="AllowDesktopSync"
type="xs:boolean" minOccurs="0" />
                                                <xs:element name="MaxCalendarAgeFilter"
type="xs:unsignedInt" minOccurs="0" />
                                                <xs:element name="AllowHTMLEmail"
type="xs:boolean" minOccurs="0" />
                                                <xs:element name="MaxEmailAgeFilter"
type="xs:unsignedInt" minOccurs="0" />
                                                <xs:element
name="MaxEmailBodyTruncationSize" type="xs:integer" minOccurs="0" />
                                                <xs:element
name="MaxEmailHTMLBodyTruncationSize" type="xs:integer" minOccurs="0" />
                                                <xs:element
name="RequireSignedSMIMEMessages" type="xs:boolean" minOccurs="0" />
                                                <xs:element
name="RequireEncryptedSMIMEMessages " type="xs:boolean" minOccurs="0" />
                                                <xs:element
name="RequireSignedSMIMEAlgorithm" type="xs:boolean" minOccurs="0" />
                                                <xs:element
name="RequireEncryptionSMIMEAlgorithm" type="xs:boolean" minOccurs="0" />
                                                <xs:element
name="AllowSMIMEEncryptionAlgorithmNegotiation" type="xs:boolean" minOccurs="0" />
                                                <xs:element name="AllowSMIMESoftCerts"
type="xs:boolean" minOccurs="0" />
                                                <xs:element name="AllowBrowser"
type="xs:boolean" minOccurs="0" />
                                                <xs:element name="AllowConsumerEmail"
type="xs:boolean" minOccurs="0" />
                                                <xs:element name="AllowRemoteDesktop"
type="xs:boolean" minOccurs="0" />
                                                <xs:element name="AllowInternetSharing"
type="xs:boolean" minOccurs="0" />
                                                <xs:element
name="UnapprovedInROMApplicationList" minOccurs="0">
                                                    <xs:complexType>
                                                        <xs:sequence>
                                                            <xs:element
name="ApplicationName" minOccurs="0" type="xs:string" />
                                                        </xs:sequence>
                                                    </xs:complexType>
```

```
                                                    </xs:element>
                                                    <xs:element name="ApprovedApplicationList"
minOccurs="0">
                                                        <xs:complexType>
                                                            <xs:sequence>
                                                                <xs:element name="Hash"
minOccurs="0" type="xs:string" />
                                                            </xs:sequence>
                                                        </xs:complexType>
                                                    </xs:element>
                                                </xs:sequence>
                                            </xs:complexType>
                                        </xs:element>
                                    </xs:sequence>
                                </xs:complexType>
                            </xs:element>
                        </xs:sequence>
                    </xs:complexType>
                </xs:element>
            </xs:sequence>
        </xs:complexType>
    </xs:element>

    <xs:element name="RemoteWipe" minOccurs="0" />
</xs:sequence>
</xs:complexType>
</xs:element>

</xs:schema>
```

2.2.1 Namespaces

This specification defines and references various **XML namespaces** using the mechanisms specified in [XMLNS]. Although this specification associates a specific XML namespace prefix for each XML namespace that is used, the choice of any particular XML namespace prefix is implementation-specific and not significant for interoperability.

Prefix	Namespace URI	Reference
provision	Provision	Section 2.2
settings	Settings	[MS-ASCMD] section 2.2.1.16
xs	http://www.w3.org/2001/XMLSchema	[XMLSCHEMA1]

2.2.2 Complex Types

The following table summarizes the set of common XML schema complex type definitions defined by this specification.

Complex Type	Description
Policies	A **collection** of security policies.
Policies.Policy	A policy.
Policies.Policy.Data	The settings for a policy.

Complex Type	Description
Policies.Policy.Data.eas-provisioningdoc	The collection of security settings for device provisioning.
Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList	A list of in-ROM applications that are not approved for execution.
Policies.Policy.Data.eas-provisioningdoc.ApprovedApplicationList	A list of in-RAM applications that are approved for execution.
RemoteWipe	A container for status information indicating client compliance with a **remote wipe** directive from the server.

2.2.2.1 Policies

The **Policies** type is a required **container** ([MS-ASDTYPE] section 2.8) type that specifies a collection of security policies.

A command response has one top-level **Policies** type per response.

The **Policies** type has only the following child element:

- **Policy** (section 2.2.2.2): At least one element of this type is required.

2.2.2.2 Policies.Policy

The **Policies.Policy** type is a required **container** ([MS-ASDTYPE] section 2.8) type that specifies a policy.

This element is valid in both a command request and a command response.

The **Policies.Policy** type has only the following child elements:

- <Policies.Policy.PolicyType> (section 2.2.3.3)
- <Policies.Policy.Status> (section 2.2.3.4)
- <Policies.Policy.PolicyKey> (section 2.2.3.5)
- **Policies.Policy.Data** (section 2.2.2.3): One instance of this element is required.

2.2.2.3 Policies.Policy.Data

The **Policies.Policy.Data** type is a required **container** ([MS-ASDTYPE] section 2.8) type that specifies the settings for a policy.

The **Policies.Policy.Data** type has only the following child element:

- **Policies.Policy.Data.eas-provisioningdoc** (section 2.2.2.4): One instance of this element is required.

2.2.2.4 Policies.Policy.Data.eas-provisioningdoc

The <Policies.Policy.Data.eas-provisioningdoc> element is a required **container** ([MS-ASDTYPE] section 2.8) element that specifies the collection of security settings for device provisioning.

A command response has a minimum of one <Policies.Policy.Data.eas-provisioningdoc> type per <Policies.Policy.Data> element.

The <Policies.Policy.Data.eas-provisioningdoc> type has only the following child elements:

- <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled> (section 2.2.3.6)
- <Policies.Policy.Data.eas-provisioningdoc.AlphaNumericDevicePasswordRequired> (section 2.2.3.7)
- <Policies.Policy.Data.eas-provisioningdoc.PasswordRecoveryEnabled> (section 2.2.3.8)
- <Policies.Policy.Data.eas-provisioningdoc.DeviceEncryptionEnabled> (section 2.2.3.9)
- <Policies.Policy.Data.eas-provisioningdoc.AttachmentsEnabled> (section 2.2.3.10)
- <Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordLength> (section 2.2.3.11)
- <Policies.Policy.Data.eas-provisioningdoc.MaxInactivityTimeDeviceLock> (section 2.2.3.12)
- <Policies.Policy.Data.eas-provisioningdoc.MaxDevicePasswordFailedAttempts> (section 2.2.3.13)
- <Policies.Policy.Data.eas-provisioningdoc.MaxAttachmentSize> (section 2.2.3.14)
- <Policies.Policy.Data.eas-provisioningdoc.AllowSimpleDevicePassword> (section 2.2.3.15)
- <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordExpiration> (section 2.2.3.16)
- <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordHistory> (section 2.2.3.17)
- <Policies.Policy.Data.eas-provisioningdoc.AllowStorageCard> (section 2.2.3.18)
- <Policies.Policy.Data.eas-provisioningdoc.AllowCamera> (section 2.2.3.19)
- <Policies.Policy.Data.eas-provisioningdoc.RequireDeviceEncryption> (section 2.2.3.20)
- <Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedApplications> (section 2.2.3.21)
- <Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedInstallationPackages> (section 2.2.3.22)
- <Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordComplexCharacters> (section 2.2.3.23)
- <Policies.Policy.Data.eas-provisioningdoc.AllowWifi> (section 2.2.3.24)
- <Policies.Policy.Data.eas-provisioningdoc.AllowTextMessaging> (section 2.2.3.25)
- <Policies.Policy.Data.eas-provisioningdoc.AllowPOPIMAPEmail> (section 2.2.3.26)
- <Policies.Policy.Data.eas-provisioningdoc.AllowBluetooth> (section 2.2.3.27)
- <Policies.Policy.Data.eas-provisioningdoc.AllowIrDA> (section 2.2.3.28)
- <Policies.Policy.Data.eas-provisioningdoc.RequireManualSyncWhenRoaming> (section 2.2.3.29)
- <Policies.Policy.Data.eas-provisioningdoc.AllowDesktopSync> (section 2.2.3.30)
- <Policies.Policy.Data.eas-provisioningdoc.MaxCalendarAgeFilter> (section 2.2.3.31)
- <Policies.Policy.Data.eas-provisioningdoc.AllowHTMLEmail> (section 2.2.3.32)

- <Policies.Policy.Data.eas-provisioningdoc.MaxEmailAgeFilter> (section 2.2.3.33)
- <Policies.Policy.Data.eas-provisioningdoc.MaxEmailBodyTruncationSize> (section 2.2.3.34)
- <Policies.Policy.Data.eas-provisioningdoc.MaxEmailHTMLBodyTruncationSize> (section 2.2.3.35)
- <Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEMessages> (section 2.2.3.36)
- <Policies.Policy.Data.eas-provisioningdoc.RequireEncryptedSMIMEMessages> (section 2.2.3.37)
- <Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEAlgorithm> (section 2.2.3.38)
- <Policies.Policy.Data.eas-provisioningdoc.RequireEncryptionSMIMEAlgorithm> (section 2.2.3.39)
- <Policies.Policy.Data.eas-provisioningdoc.AllowSMIMEEncryptionAlgorithmNegotiation> (section 2.2.3.40)
- <Policies.Policy.Data.eas-provisioningdoc.AllowSMIMESoftCerts> (section 2.2.3.41)
- <Policies.Policy.Data.eas-provisioningdoc.AllowBrowser> (section 2.2.3.42)
- <Policies.Policy.Data.eas-provisioningdoc.AllowConsumerEmail> (section 2.2.3.43)
- <Policies.Policy.Data.eas-provisioningdoc.AllowRemoteDesktop> (section 2.2.3.44)
- <Policies.Policy.Data.eas-provisioningdoc.AllowInternetSharing> (section 2.2.3.45)
- <Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList> (section 2.2.2.5)
- <Policies.Policy.Data.eas-provisioningdoc.ApprovedApplicationList> (section 2.2.2.6)

2.2.2.5 Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList

The **Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList** type is an optional **container** ([MS-ASDTYPE] section 2.8) element that specifies a list of in-ROM applications that are not approved for execution. Only applications that are preinstalled in ROM are affected by the entries in this element. This element does not apply to applications that are installed in-memory.

A command response has a maximum of one **Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList** type per **Policies.Policy.Data.eas-provisioningdoc** type.

The **Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList** type has only the following child elements:

- <Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList.ApplicationName> (Section 2.2.3.46): This element is optional.

2.2.2.6 Policies.Policy.Data.eas-provisioningdoc.ApprovedApplicationList

The **Policies.Policy.Data.eas-provisioningdoc.ApprovedApplicationList** element is an optional **container** ([MS-ASDTYPE] section 2.8) element that specifies a list of in-memory applications that are approved for execution. Only in-memory applications are affected by this element. This element does not apply to in-ROM applications. If present, the client MUST only allow the in-memory applications specified by this element to execute.

A command response has a maximum of one **Policies.Policy.Data.eas-provisioningdoc.ApprovedApplicationList** type per <Policies.Policy.Data.eas-provisioningdoc> element.

The **Policies.Policy.Data.eas-provisioningdoc.ApprovedApplicationList** type has only the following child elements:

- <Policies.Policy.Data.eas-provisioningdoc.ApprovedApplicationList.Hash> (section 2.2.3.47): This element is optional.

2.2.2.7 RemoteWipe

The **RemoteWipe** type is an optional **container** ([MS-ASDTYPE] section 2.8) type that specifies the result of a remote wipe directive from the server.

The **RemoteWipe** type is sent in a command request by the client only in response to a remote wipe directive from the server.

The **RemoteWipe** type has the following child element:

- **Status** (section 2.2.3.49): One element of this type is required in a remote wipe client request.

2.2.3 Elements

The following table summarizes the set of common XML schema element definitions that are defined or used by this specification. XML schema elements that are specific to a particular command are described in the context of its associated command.

Element	Description
<settings:DeviceInformation>	Specifies the settings for the device in an initial Provisioning request.
<Status>	Indicates whether the **Provision** command was handled correctly.
<Policies.Policy.PolicyType>	Specifies the format in which the policy settings are to be provided.
<Policies.Policy.Status>	Indicates whether the policy settings were applied correctly.
<Policies.Policy.PolicyKey>	Used by the server to mark the state of policy settings on the client.
<Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled>	Indicates whether a client device requires a password.
<Policies.Policy.Data.eas-provisioningdoc.AlphaNumericDevicePasswordRequired>	Indicates whether a client device requires an AlphaNumeric password.
<Policies.Policy.Data.eas-provisioningdoc.PasswordRecoveryEnabled>	Indicates whether to enable a recovery password to be sent

Element	Description
	to the server by using the **Settings** command.
<Policies.Policy.Data.eas-provisioningdoc.DeviceEncryptionEnabled>	Indicates whether the device has to encrypt content that is stored on the **storage** card.
<Policies.Policy.Data.eas-provisioningdoc.AttachmentsEnabled>	Indicates whether e-mail **attachments** are enabled.
<Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordLength>	The minimum device password length that the user can enter.
<Policies.Policy.Data.eas-provisioningdoc.MaxInactivityTimeDeviceLock>	The number of seconds of inactivity before the device locks itself.
<Policies.Policy.Data.eas-provisioningdoc.MaxDevicePasswordFailedAttempts>	The number of password failures that are permitted before the device is wiped.
<Policies.Policy.Data.eas-provisioningdoc.MaxAttachmentSize>	The maximum attachment size, as determined by the security policy.
<Policies.Policy.Data.eas-provisioningdoc.AllowSimpleDevicePassword>	Whether the device allows simple passwords.
<Policies.Policy.Data.eas-provisioningdoc.DevicePasswordExpiration>	Whether the password expires after the specified number of days, as determined by the policy.
<Policies.Policy.Data.eas-provisioningdoc.DevicePasswordHistory>	The minimum number of previously used passwords the client device stores to prevent reuse.
<Policies.Policy.Data.eas-provisioningdoc.AllowStorageCard>	Whether the device allows the use of the storage card.
<Policies.Policy.Data.eas-provisioningdoc.AllowCamera>	Whether the device allows the use of the built-in camera.
<Policies.Policy.Data.eas-provisioningdoc.RequireDeviceEncryption>	Whether the device uses encryption.
<Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedApplications>	Whether the device allows unsigned applications to execute.
<Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedInstallationPackages>	Whether the device allows unsigned **cabinet files** to be installed.
<Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordComplexCharacters>	The minimum number of complex characters (numbers and symbols) contained within

Element	Description
	the password.
<Policies.Policy.Data.eas-provisioningdoc.AllowWiFi>	Whether the device allows the use of WiFi connections.
<Policies.Policy.Data.eas-provisioningdoc.AllowTextMessaging>	Whether the device allows **Short Message Service (SMS)**/text messaging.
<Policies.Policy.Data.eas-provisioningdoc.AllowPOPIMAPEmail>	Whether the device allows access to POP/IMAP e-mail.
<Policies.Policy.Data.eas-provisioningdoc.AllowBluetooth>	Whether Bluetooth and hands-free profiles are allowed on the device.
<Policies.Policy.Data.eas-provisioningdoc.AllowIrDA>	Whether the device allows the use of IrDA (infrared) connections.
<Policies.Policy.Data.eas-provisioningdoc.RequireManualSyncWhenRoaming>	Whether the device requires manual **synchronization** when the device is roaming.
<Policies.Policy.Data.eas-provisioningdoc.AllowDesktopSync>	Whether the device allows synchronization with Desktop ActiveSync.
<Policies.Policy.Data.eas-provisioningdoc.MaxCalendarAgeFilter>	The maximum number of **calendar** days that can be synchronized.
<Policies.Policy.Data.eas-provisioningdoc.AllowHTMLEmail>	Whether the device uses **HTML**-formatted e-mail.
<Policies.Policy.Data.eas-provisioningdoc.MaxEmailAgeFilter>	The e-mail age limit for synchronization.
<Policies.Policy.Data.eas-provisioningdoc.MaxEmailBodyTruncationSize>	The truncation size for **plain text**–formatted e-mail **messages**.
<Policies.Policy.Data.eas-provisioningdoc.MaxEmailHTMLBodyTruncationSize>	The truncation size for HTML-formatted e-mail messages.
<Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEMessages>	Whether the device is required to send signed S/MIME messages.
<Policies.Policy.Data.eas-provisioningdoc.RequireEncryptedSMIMEMessages>	Whether the device is required to send **encrypted S/MIME messages**.
<Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEAlgorithm>	The algorithm to be used when signing a message.
<Policies.Policy.Data.eas-provisioningdoc.RequireEncryptionSMIMEAlgorithm>	The algorithm to be used when encrypting a message.

Element	Description
<Policies.Policy.Data.eas-provisioningdoc.AllowSMIMEEncryptionAlgorithmNegotiation>	Whether the device can negotiate the encryption algorithm to be used for signing.
<Policies.Policy.Data.eas-provisioningdoc.AllowSMIMESoftCerts>	Whether the device uses soft certificates to sign outgoing messages.
<Policies.Policy.Data.eas-provisioningdoc.AllowBrowser>	Whether the device allows the use of a Web browser.
<Policies.Policy.Data.eas-provisioningdoc.AllowConsumerEmail>	Whether the device allows the use of Windows Live.
<Policies.Policy.Data.eas-provisioningdoc.AllowRemoteDesktop>	Whether the device allows the use of Remote Desktop.
<Policies.Policy.Data.eas-provisioningdoc.AllowInternetSharing>	Whether the device allows the use of Internet Sharing.
<Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList.ApplicationName>	The name of an in-ROM application (.exe file) that is not approved for execution.
<Policies.Policy.Data.eas-provisioningdoc.ApprovedApplicationList.Hash>	The SHA-1 hash of an in-memory application that is approved for execution.
RemoteWipe	A remote wipe directive from the server in a command response.
RemoteWipe.Status	The status returned by the client in a command request to a remote wipe directive from the server.

2.2.3.1 DeviceInformation

The <settings:DeviceInformation> element is an optional container node that is used for sending the client device's properties to the server in an initial **Provision** command request. The <settings:DeviceInformation> element is defined in the Settings XML namespace, as specified in [MS-ASCMD] section 2.2.1.16.1.

A client SHOULD send the <settings:DeviceInformation> element with its contents when sending an initial **Provision** command request to the server but not on subsequent requests.<1>

When the **Provision** command is used to send the <settings:DeviceInformation> element, it sends the information about the client device to the server, as specified for the <settings:DeviceInformation> element under the **Settings** command in [MS-ASCMD] section 2.2.1.16.1.15.

2.2.3.2 Status

The <Status> element indicates success or failure of the command in multiple locations in the command request and response. The <Status> element that is returned as a direct child of the <Provision> element in a command response indicates whether the **Provision** command was handled correctly.

The following table lists valid values for the <Status> element.

Value	Meaning
1	Success
2	Protocol error
3	General server error
4	The device is externally managed

2.2.3.3 Policies.Policy.PolicyType

In the download policy settings phase, the <PolicyType> element specifies the format in which the policy settings are to be provided to the client device.

<PolicyType> MUST be MS-EAS-Provisioning-WBXML.

2.2.3.4 Policies.Policy.Status

The <Status> element indicates success or failure of the command in two different locations in the response. The <Status> element that is returned as a child of a <Policies.Policy> element indicates whether the policy settings were applied correctly.

The following table lists valid values for the <Status> element as a child of the <Policies.Policy> element in the response from the server to the client.

Value	Meaning
1	Success.
2	There is no policy for this client.
3	Unknown <PolicyType> value.
4	The policy data on the server is corrupted (possibly tampered with).
5	The client is acknowledging the wrong **policy key**.

The following table lists valid values for the <Status> element as a child of the <Policy> element in the response from the client to the server.

Value	Meaning
1	Success
2	Partial success (at least the PIN was enabled).

Value	Meaning
3	The client did not apply the policy at all.
4	The client claims to have been provisioned by a third party.

2.2.3.5 Policies.Policy.PolicyKey

<PolicyKey> is an optional element of type **string** with a maximum of 64 characters and no child elements.

<PolicyKey> is used by the server to mark the state of policy settings on the client in the settings download phase of the **Provision** command. In the acknowledgement phase, the <PolicyKey> element is used by the client and server to correlate acknowledgements to a particular policy setting.

The <PolicyKey> element is a random unique unsigned **integer**. When the client issues an initial **Provision** command, the <PolicyKey> tag and X-MS-PolicyKey is not included in the **HTTP header**.

2.2.3.6 Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled

The <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled> element is a required child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether a device requires a password.

The **Policies.Policy.Data.eas-provisioningdoc** type has one instance of the <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled> element.

The <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled> are listed in the following table.

Value	Description
0	Device password is not required.
1	Device password is required.

2.2.3.7 Policies.Policy.Data.eas-provisioningdoc.AlphaNumericDevicePasswordRequired

The <Policies.Policy.Data.eas-provisioningdoc.AlphaNumericDevicePasswordRequired> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether a device requires an alphanumeric password.

The <Policies.Policy.Data.eas-provisioningdoc.AlphaNumericDevicePasswordRequired> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AlphaNumericDevicePasswordRequired> are listed in the following table.

Value	Description
0	Alphanumeric device password is not required.
1	Alphanumeric device password is required.

If <Policies.Policy.Data.eas-provisioningdoc.AlphaNumericDevicePasswordRequired> is not included in a response, a client SHOULD treat this value as 0.

If the <Policies.Policy.Data.eas-provisioningdoc.AlphaNumericDevicePasswordRequired> element is included in a response, and <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled> is FALSE (0), the client ignores this element.

2.2.3.8 Policies.Policy.Data.eas-provisioningdoc.PasswordRecoveryEnabled

The <Policies.Policy.Data.eas-provisioningdoc.PasswordRecoveryEnabled> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the server supports storage of a recovery password to be sent by the client using the **Settings** command.

The <Policies.Policy.Data.eas-provisioningdoc.PasswordRecoveryEnabled> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.PasswordRecoveryEnabled> are listed in the following table.

Value	Description
0	Password recovery is not enabled on the server.
1	Password recovery is enabled on the server.

A recovery password is a special password created by the device that gives the administrator or user the ability to log on to the device one time, after which the user is required to create a new password. The device then creates a new recovery password. If the <Policies.Policy.Data.eas-provisioningdoc.PasswordRecoveryEnabled> element is set to 1 (TRUE), the server supports storage of a recovery password sent by the device. If the element is set to 0 (FALSE), the device SHOULD NOT send a recovery password, because the server does not support storage of the password.

If <Policies.Policy.Data.eas-provisioningdoc.PasswordRecoveryEnabled> is not included in a response, a client SHOULD treat this value as 0.

If the <Policies.Policy.Data.eas-provisioningdoc.PasswordRecoveryEnabled> element is included in a response, and <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled> is FALSE (0), the client SHOULD ignore this element.

2.2.3.9 Policies.Policy.Data.eas-provisioningdoc.DeviceEncryptionEnabled

The <Policies.Policy.Data.eas-provisioningdoc.DeviceEncryptionEnabled> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device encrypts content that is stored on the device.

The <Policies.Policy.Data.eas-provisioningdoc.DeviceEncryptionEnabled> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.DeviceEncryptionEnabled> are listed in the following table.

Value	Description
0	Device encryption is not required.
1	Device encryption is required.

2.2.3.10 Policies.Policy.Data.eas-provisioningdoc.AttachmentsEnabled

The <Policies.Policy.Data.eas-provisioningdoc.AttachmentsEnabled> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether e-mail attachments are enabled.

The <Policies.Policy.Data.eas-provisioningdoc.AttachmentsEnabled> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AttachmentsEnabled> are listed in the following table.

Value	Description
0	Attachments are not allowed.
1	Attachments are allowed.

2.2.3.11 Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordLength

The <Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordLength> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies the minimum device password length that the user can enter.

The <Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordLength> element cannot have child elements.

<Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordLength> is an **integer**. <Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordLength> MUST have a value no less than 1 and no greater than 16. If the value of this element is 1, there is no minimum length for the device password.

If the <Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordLength> element is included in a response, and **Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled** is FALSE (0), the client SHOULD ignore this element.

2.2.3.12 Policies.Policy.Data.eas-provisioningdoc.MaxInactivityTimeDeviceLock

The <Policies.Policy.Data.eas-provisioningdoc.MaxInactivityTimeDeviceLock> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies the maximum number of seconds of inactivity before the device locks itself.

The <Policies.Policy.Data.eas-provisioningdoc.MaxInactivityTimeDeviceLock> element cannot have child elements.

<Policies.Policy.Data.eas-provisioningdoc.MaxInactivityTimeDeviceLock> is an **integer**. If this value is greater than or equal to 9999, the client interprets it as unlimited.

If the <Policies.Policy.Data.eas-provisioningdoc.MaxInactivityTimeDeviceLock> element is not included in a response, the client interprets this as meaning that no time device lock has been set by the security policy.

2.2.3.13 Policies.Policy.Data.eas-provisioningdoc.MaxDevicePasswordFailedAttempts

The <Policies.Policy.Data.eas-provisioningdoc.MaxDevicePasswordFailedAttempts> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies the maximum number of failed password logon attempts that are permitted before the device SHOULD perform a local wipe or enter a timed lock out mode.

The <Policies.Policy.Data.eas-provisioningdoc.MaxDevicePasswordFailedAttempts> element cannot have child elements.

<Policies.Policy.Data.eas-provisioningdoc.MaxDevicePasswordFailedAttempts> is an **integer** with a value in the range from 4 through 16.

If the <Policies.Policy.Data.eas-provisioningdoc.MaxDevicePasswordFailedAttempts> element is included in a response, and the <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled> element is set to FALSE (0), the client ignores this element.

2.2.3.14 Policies.Policy.Data.eas-provisioningdoc.MaxAttachmentSize

The <Policies.Policy.Data.eas-provisioningdoc.MaxAttachmentSize> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies the maximum attachment size in bytes as determined by security policy.

The **Policies.Policy.Data.eas-provisioningdoc** type has one instance of the <Policies.Policy.Data.eas-provisioningdoc.MaxAttachmentSize> element.

The <Policies.Policy.Data.eas-provisioningdoc.MaxAttachmentSize> element cannot have child elements.

<Policies.Policy.Data.eas-provisioningdoc.MaxAttachmentSize> is an **integer**.

2.2.3.15 Policies.Policy.Data.eas-provisioningdoc.AllowSimpleDevicePassword

The <Policies.Policy.Data.eas-provisioningdoc.AllowSimpleDevicePassword> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows simple passwords. A simple password is one consisting only of repeated ("2222") or sequential ("abcd") characters.

The <Policies.Policy.Data.eas-provisioningdoc.AllowSimpleDevicePassword> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowSimpleDevicePassword> are listed in the following table.

Value	Description
0	Simple passwords are not allowed.

Value	Description
1	Simple passwords are allowed.

If <Policies.Policy.Data.eas-provisioningdoc.AllowSimpleDevicePassword> is not included in a response, a client SHOULD treat this value as 1.

If the <Policies.Policy.Data.eas-provisioningdoc.AllowSimpleDevicePassword> element is included in a response, and the <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled> element is set to FALSE (0), the client SHOULD ignore this element.

2.2.3.16 Policies.Policy.Data.eas-provisioningdoc.DevicePasswordExpiration

The <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordExpiration> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies the maximum number of days until a password expires.

The <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordExpiration> element can be empty, indicating that no device password expiration policy is set.

The <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordExpiration> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordExpiration> are listed in the following table.

Value	Description
0	Passwords do not expire.
>0	Passwords expire in the specified maximum number of days.

If <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordExpiration> is empty or is not included in a response, a client SHOULD treat this value as 0.

If the <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordExpiration> element is included in a response, and the <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled> element is set to FALSE (0), the client SHOULD ignore this element.

2.2.3.17 Policies.Policy.Data.eas-provisioningdoc.DevicePasswordHistory

The <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordHistory> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies the minimum number of previously used passwords stored to prevent reuse on the client device.

The <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordHistory> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordHistory> are listed in the following table.

Value	Description
0	Storage of previously used passwords is not required.

Value	Description
>0	The minimum number of previously used passwords to be stored.

If <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordHistory> is not included in a response, then a client SHOULD treat this value as 0.

If the value of the <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordHistory> element is greater than 0, and the value of the <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled> element is set to TRUE (1), the client disallows the user from using a stored prior password after a password expires.

If the <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordHistory> element is included in a response, and the <Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled> element is set to FALSE (0), the client SHOULD ignore this element.

2.2.3.18 Policies.Policy.Data.eas-provisioningdoc.AllowStorageCard

The <Policies.Policy.Data.eas-provisioningdoc.AllowStorageCard> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows use of the storage card.

The <Policies.Policy.Data.eas-provisioningdoc.AllowStorageCard> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowStorageCard> are listed in the following table.

Value	Description
0	SD card use is not allowed.
1	SD card use is allowed.

2.2.3.19 Policies.Policy.Data.eas-provisioningdoc.AllowCamera

The <Policies.Policy.Data.eas-provisioningdoc.AllowCamera> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows the use of the built-in camera.

The <Policies.Policy.Data.eas-provisioningdoc.AllowCamera> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowCamera> are listed in the following table.

Value	Description
0	Use of the camera is not allowed.
1	Use of the camera is allowed.

2.2.3.20 Policies.Policy.Data.eas-provisioningdoc.RequireDeviceEncryption

The <Policies.Policy.Data.eas-provisioningdoc.RequireDeviceEncryption> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device uses encryption.

The <Policies.Policy.Data.eas-provisioningdoc.RequireDeviceEncryption> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.RequireDeviceEncryption> are listed in the following table.

Value	Description
0	Encryption is not required.
1	Encryption is required.

2.2.3.21 Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedApplications

The <Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedApplications> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows unsigned applications to execute.

The <Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedApplications> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedApplications> are listed in the following table.

Value	Description
0	Unsigned applications are not allowed to execute.
1	Unsigned applications are allowed to execute.

2.2.3.22 Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedInstallationPackages

The <Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedInstallationPackages> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows unsigned cabinet files to be installed.

The <Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedInstallationPackages> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedInstallationPackages> are listed in the following table.

Value	Description
0	Unsigned cabinet files are not allowed to be installed.
1	Unsigned cabinet files are allowed to be installed.

2.2.3.23 Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordComplexCharacters

The <Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordComplexCharacters> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies the minimum number of complex characters (numbers and symbols) that the device password must contain.

The <Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordComplexCharacters> element cannot have child elements.

<Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordComplexCharacters> is an **integer**. Valid values for <Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordComplexCharacters> are 1 to 4.

2.2.3.24 Policies.Policy.Data.eas-provisioningdoc.AllowWifi

The <Policies.Policy.Data.eas-provisioningdoc.AllowWifi> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows the use of Wi-Fi connections.

The <Policies.Policy.Data.eas-provisioningdoc.AllowWifi> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowWifi> are listed in the following table.

Value	Description
0	The use of Wi-Fi connections is not allowed.
1	The use of Wi-Fi connections is allowed.

2.2.3.25 Policies.Policy.Data.eas-provisioningdoc.AllowTextMessaging

The <Policies.Policy.Data.eas-provisioningdoc.AllowTextMessaging> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows the use of SMS or text messaging.

The <Policies.Policy.Data.eas-provisioningdoc.AllowTextMessaging> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowTextMessaging> are listed in the following table.

Value	Description
0	SMS or text messaging is not allowed.
1	SMS or text messaging is allowed.

2.2.3.26 Policies.Policy.Data.eas-provisioningdoc.AllowPOPIMAPEmail

The <Policies.Policy.Data.eas-provisioningdoc.AllowPOPIMAPEmail> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows access to POP or IMAP e-mail.

The <Policies.Policy.Data.eas-provisioningdoc.AllowPOPIMAPEmail> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowPOPIMAPEmail> are listed in the following table.

Value	Description
0	POP or IMAP e-mail access is not allowed.
1	POP or IMAP e-mail access is allowed.

2.2.3.27 Policies.Policy.Data.eas-provisioningdoc.AllowBluetooth

The <Policies.Policy.Data.eas-provisioningdoc.AllowBluetooth> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies the use of Bluetooth on the device.

The <Policies.Policy.Data.eas-provisioningdoc.AllowBluetooth> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowBluetooth> are listed in the following table.

Value	Description
0	Disable Bluetooth.
1	Disable Bluetooth, but allow the configuration of hands-free profiles.
2	Allow Bluetooth.

2.2.3.28 Policies.Policy.Data.eas-provisioningdoc.AllowIrDA

The <Policies.Policy.Data.eas-provisioningdoc.AllowIrDA> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows the use of IrDA (infrared) connections.

The <Policies.Policy.Data.eas-provisioningdoc.AllowIrDA> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowIrDA> are listed in the following table.

Value	Description
0	Disable IrDA.
1	Allow IrDA.

2.2.3.29 Policies.Policy.Data.eas-provisioningdoc.RequireManualSyncWhenRoaming

The <Policies.Policy.Data.eas-provisioningdoc.RequireManualSyncWhenRoaming> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device requires manual synchronization when the device is roaming.

The <Policies.Policy.Data.eas-provisioningdoc.RequireManualSyncWhenRoaming> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.RequireManualSyncWhenRoaming> are listed in the following table.

Value	Description
0	Do not require manual sync; allow direct push when roaming.
1	Require manual sync when roaming.

2.2.3.30 Policies.Policy.Data.eas-provisioningdoc.AllowDesktopSync

The <Policies.Policy.Data.eas-provisioningdoc.AllowDesktopSync> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows synchronization with Desktop ActiveSync.

The <Policies.Policy.Data.eas-provisioningdoc.AllowDesktopSync> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowDesktopSync> are listed in the following table.

Value	Description
0	Do not allow Desktop ActiveSync.
1	Allow Desktop ActiveSync.

2.2.3.31 Policies.Policy.Data.eas-provisioningdoc.MaxCalendarAgeFilter

The <Policies.Policy.Data.eas-provisioningdoc.MaxCalendarAgeFilter> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies the maximum number of calendar days that can be synchronized.

The <Policies.Policy.Data.eas-provisioningdoc.MaxCalendarAgeFilter> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.MaxCalendarAgeFilter> are listed in the following table.

Value	Description
0	All days
4	2 weeks
5	1 month
6	3 months
7	6 months

2.2.3.32 Policies.Policy.Data.eas-provisioningdoc.AllowHTMLEmail

The <Policies.Policy.Data.eas-provisioningdoc.AllowHTMLEmail> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device uses HTML-formatted e-mail.

The <Policies.Policy.Data.eas-provisioningdoc.AllowHTMLEmail> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowHTMLEmail> are listed in the following table.

Value	Description
0	HTML-formatted e-mail is not allowed.
1	HTML-formatted e-mail is allowed.

2.2.3.33 Policies.Policy.Data.eas-provisioningdoc.MaxEmailAgeFilter

The <Policies.Policy.Data.eas-provisioningdoc.MaxEmailAgeFilter> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies the e-mail age limit for synchronization.

The <Policies.Policy.Data.eas-provisioningdoc.MaxEmailAgeFilter> element cannot have child elements.

Valid values are listed in the following table and represent the maximum allowable number of days to sync e-mail.

Value	Description
0	Sync all
1	1 day
2	3 days
3	1 week
4	2 weeks
5	1 month

2.2.3.34 Policies.Policy.Data.eas-provisioningdoc.MaxEmailBodyTruncationSize

The <Policies.Policy.Data.eas-provisioningdoc.MaxEmailBodyTruncationSize> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies the truncation size for plain text–formatted e-mail.

The <Policies.Policy.Data.eas-provisioningdoc.MaxEmailBodyTruncationSize> element cannot have child elements.

Valid values for the <Policies.Policy.Data.eas-provisioningdoc.MaxEmailBodyTruncationSize> element MUST be an **integer** of one of the values or ranges listed in the following table.

Value	Description
-1	No truncation.
0	Truncate only the header.
>0	Truncate the e-mail body to the specified size.

2.2.3.35 Policies.Policy.Data.eas-provisioningdoc.MaxEmailHTMLBodyTruncationSize

The <Policies.Policy.Data.eas-provisioningdoc.MaxEmailHTMLBodyTruncationSize> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies the truncation size for HTML-formatted e-mail.

The <Policies.Policy.Data.eas-provisioningdoc.MaxEmailHTMLBodyTruncationSize> element cannot have child elements.

Valid values for the <Policies.Policy.Data.eas-provisioningdoc.MaxEmailHTMLBodyTruncationSize> element are an **integer** of one of the values or ranges listed in the following table.

Value	Description
-1	No truncation.
0	Truncate only the header.
>0	Truncate the e-mail body to the specified size.

2.2.3.36 Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEMessages

The <Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEMessages> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device sends signed S/MIME messages.

The <Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEMessages> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEMessages> are listed in the following table.

Value	Description
0	Signed S/MIME messages are not required.
1	Signed S/MIME messages are required.

2.2.3.37 Policies.Policy.Data.eas-provisioningdoc.RequireEncryptedSMIMEMessages

The <Policies.Policy.Data.eas-provisioningdoc.RequireEncryptedSMIMEMessages> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device sends encrypted e-mail messages.

The <Policies.Policy.Data.eas-provisioningdoc.RequireEncryptedSMIMEMessages> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.RequireEncryptedSMIMEMessages> are listed in the following table.

Value	Description
0	Encrypted e-mail messages are not required.
1	E-mail messages are required to be encrypted.

2.2.3.38 Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEAlgorithm

The <Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEAlgorithm> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies the algorithm used when signing S/MIME messages.

The <Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEAlgorithm> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEAlgorithm> are listed in the following table.

Value	Description
0	Use SHA1.
1	Use MD5.

2.2.3.39 Policies.Policy.Data.eas-provisioningdoc.RequireEncryptionSMIMEAlgorithm

The <Policies.Policy.Data.eas-provisioningdoc.RequireEncryptionSMIMEAlgorithm> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies the algorithm used when encrypting S/MIME messages.

The <Policies.Policy.Data.eas-provisioningdoc.RequireEncryptionSMIMEAlgorithm> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.RequireEncryptionSMIMEAlgorithm> are listed in the following table.

Value	Description
0	TripleDES algorithm
1	DES algorithm
2	RC2128bit
3	RC264bit
4	RC240bit

2.2.3.40 Policies.Policy.Data.eas-provisioningdoc.AllowSMIMEEncryptionAlgorithmNegotiation

The <Policies.Policy.Data.eas-provisioningdoc.AllowSMIMEEncryptionAlgorithmNegotation> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that controls negotiation of the encryption algorithm.

The <Policies.Policy.Data.eas-provisioningdoc.AllowSMIMEEncryptionAlgorithmNegotation> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowSMIMEEncryptionAlgorithmNegotation> are listed in the following table.

Value	Description
0	Do not negotiate.
1	Negotiate a strong algorithm.
2	Negotiate any algorithm.

2.2.3.41 Policies.Policy.Data.eas-provisioningdoc.AllowSMIMESoftCerts

The <Policies.Policy.Data.eas-provisioningdoc.AllowSMIMESoftCerts> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device can use soft certificates to sign outgoing messages.

The <Policies.Policy.Data.eas-provisioningdoc.AllowSMIMESoftCerts> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowSMIMESoftCerts> are listed in the following table.

Value	Description
0	Soft certificates are not allowed.
1	Soft certificates are allowed.

2.2.3.42 Policies.Policy.Data.eas-provisioningdoc.AllowBrowser

The <Policies.Policy.Data.eas-provisioningdoc.AllowBrowser> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows the use of a Web browser.

The <Policies.Policy.Data.eas-provisioningdoc.AllowBrowser> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowBrowser> are listed in the following table.

Value	Description
0	Do not allow the use of a Web browser.
1	Allow the use of a Web browser.

2.2.3.43 Policies.Policy.Data.eas-provisioningdoc.AllowConsumerEmail

The <Policies.Policy.Data.eas-provisioningdoc.AllowConsumerEmail> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows the user to configure a personal e-mail account.

The <Policies.Policy.Data.eas-provisioningdoc.AllowConsumerEmail> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowConsumerEmail> are listed in the following table.

Value	Description
0	Do not allow the user to configure a personal e-mail account.
1	Allow the user to configure a personal e-mail account.

2.2.3.44 Policies.Policy.Data.eas-provisioningdoc.AllowRemoteDesktop

The <Policies.Policy.Data.eas-provisioningdoc.AllowRemoteDesktop> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows the use of Remote Desktop.

The <Policies.Policy.Data.eas-provisioningdoc.AllowRemoteDesktop> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowRemoteDesktop> are listed in the following table.

Value	Description
0	Do not allow the use of Remote Desktop.
1	Allow the use of Remote Desktop.

2.2.3.45 Policies.Policy.Data.eas-provisioningdoc.AllowInternetSharing

The <Policies.Policy.Data.eas-provisioningdoc.AllowInternetSharing> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc** type that specifies whether the device allows the use of Internet Sharing.

The <Policies.Policy.Data.eas-provisioningdoc.AllowInternetSharing> element cannot have child elements.

Valid values for <Policies.Policy.Data.eas-provisioningdoc.AllowInternetSharing> are listed in the following table.

Value	Description
0	Do not allow the use of Internet Sharing.
1	Allow the use of Internet Sharing.

2.2.3.46 Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList.ApplicationName

The <Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList.ApplicationName> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList** type that specifies the name of an in-ROM application (.exe file) that is not approved for execution. Only in-ROM applications are valid values for this element. In-memory applications MUST be ignored.

The **Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList** type has at least one **instance** of the <Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList.ApplicationName> element.

There is no limit on the number of <Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList.ApplicationName> elements that are defined for a **Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList** type.

2.2.3.47 Policies.Policy.Data.eas-provisioningdoc.ApprovedApplicationList.Hash

The <Policies.Policy.Data.eas-provisioningdoc.ApprovedApplicationList.Hash> element is an optional child element of the **Policies.Policy.Data.eas-provisioningdoc.ApprovedApplicationList** type that specifies the SHA1 hash of an approved in-memory application. Only SHA1 hashes of in-memory applications are valid values for this element. SHA1 hashes of in-ROM applications MUST be ignored.

There is no limit on the number of <Policies.Policy.Data.eas-provisioningdoc.ApprovedApplicationList.Hash> elements that are defined for a **Policies.Policy.Data.eas-provisioningdoc.ApprovedApplicationList** type.

2.2.3.48 RemoteWipe

The <RemoteWipe> element is an optional child element of the <Provision> element in a server command response that specifies the client is to execute a remote wipe operation.

The server MUST send one empty <RemoteWipe> element when specifying the client is to execute a remote wipe operation. The <RemoteWipe> element MUST be omitted from a command response otherwise.

2.2.3.49 RemoteWipe.Status

The <Status> element sent as a child of a **RemoteWipe** type in a command request indicates the success or failure of a remote wipe operation on the client following a remote wipe directive from the server. The <Status> element is a required child element of the **RemoteWipe** type sent in a command request.

The **RemoteWipe** type in a command request MUST contain one <Status> element. The <Status> element cannot have child elements.

Valid values for the <Status> element are listed in the following table.

Value	Description
1	The client remote wipe operation was successful
2	The remote wipe operation failed

3 Protocol Details

3.1 Client Details

3.1.1 Abstract Data Model

This section describes a conceptual model of possible data organization that an implementation maintains to participate in this protocol. The described organization is provided to facilitate the explanation of how the protocol behaves. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with that described in this document.

3.1.2 Timers

None.

3.1.3 Initialization

None.

3.1.4 Higher-Layer Triggered Events

None.

3.1.5 Message Processing Events and Sequencing Rules

3.1.5.1 Provision Command

The **Provision** command enables client devices to send the server information about the device, to request from the server the security policy settings set by the server administrator, and to report on the status of a remote wipe directive.

The **Provision** command has two phases: an initial phase consisting of a client request followed by an initial server response, then an acknowledgment phase consisting of a client request with an acknowledgment of the initial server response, followed by another server response.

The client ensures that the security policy settings are actually enforced. The server SHOULD require that the client device has requested and acknowledged the security policy settings before the client is allowed to synchronize with the server, unless a security policy is set on the server to allow it. The server relies on the client to apply the security policy settings on the client device.

The current security policy settings on the client are represented by a policy key, which SHOULD be sent to the server in the X-MS-PolicyKey field of the HTTP header of all protocol command requests except for the initial **Provision** command, the **Ping** command ([MS-ASCMD] section 2.2.1.11), and the **HTTP OPTIONS** command ([MS-ASHTTP] section 2.2.3). If the server returns a status code<2> in a command response indicating that the policy key of the client is out of date, the client issues a new **Provision** command to obtain the security policy settings and a new policy key.

Note that the only policy key that the client can successfully use is a 0 on an initial request, or the value that it obtained from the <PolicyKey> element (section 2.2.3.5) of the most recent server response to a **Provision** command request. The <PolicyKey> value from an initial **Provision** command request for policy settings is temporary and can only be used in an acknowledgment

phase **Provision** command request. The server response to this request includes a policy key that can be used for subsequent commands.

Clients SHOULD send a **Provision** command request when first contacting the server to send device information, to obtain security policy settings, and to obtain a policy key for use in subsequent command requests. Clients SHOULD NOT send the **Provision** command again until receiving a status code<3> from the server indicating that it is necessary.

Clients SHOULD include a security policy settings request in a **Provision** command request when first contacting the server and after receiving a status code<4> from the server indicating that the policy key is out of date. A security policy settings request consists of a <PolicyType> element (section 2.2.3.3) with a value of MS-EAS-Provisioning-WBXML, contained within a **Policy** type (section 2.2.2.2), within a **Policies** type (section 2.2.2.1), within the <Provision> element in the XML body of the command request. Clients SHOULD NOT include a security policy settings request after receiving a status code from the server indicating that a remote wipe is requested.

Clients include a security policy settings acknowledgment in the **Provision** command request sent immediately following the server response to a server policy settings request. A security policy settings acknowledgment consists of a <PolicyType> element with a value of MS-EAS-Provisioning-WBXML and a <Status> element (section 2.2.3.4) with the client status value, contained within a **Policy** type, within a **Policies** type, within the <Provision> element in the XML body of the command request.

Clients SHOULD<5> include a <settings:DeviceInformation> element (specified in [MS-ASCMD] section 2.2.1.16.1) in the first **Provision** command request sent to the server and SHOULD NOT include it in subsequent **Provision** command requests.

Clients include a remote wipe acknowledgment in the **Provision** command request sent immediately following a server response that includes a <RemoteWipe> element<6> (section 2.2.3.48) within the <Provision> element in the XML body of the command response. A remote wipe acknowledgment consists of a **RemoteWipe** type (section 2.2.2.7) containing a <Status> element (section 2.2.3.49) with the client's remote wipe status value, contained within the **Provision** element in the XML body of the command request.

3.1.5.2 Provision Command Errors

Code	Meaning	Cause	Scope	Resolution
1	Success.	The requested policy data is included in the response.	Policy	Apply the policy.
2	Protocol error.	Syntax error in the Provision command request.	Global	Fix bug in client code.
2	Policy not defined.	No policy of the requested type is defined on the server.	Policy	Stop sending policy information. No policy is implemented.
3	The policy type is unknown.	The client sent a policy that the server does not recognize.	Policy	Issue a request by using MS-EAS-Provisioning-WBXML.
3	An error occurred on the server.	Server misconfiguration, temporary system issue, or bad item. This is frequently a transient condition.	Global	Retry.
5	Policy key	The client is trying to acknowledge an	Policy	Issue a new **Provision**

Code	Meaning	Cause	Scope	Resolution
	mismatch.	out-of-date or invalid policy.		request to obtain a valid policy key.

3.1.6 Timer Events

None.

3.1.7 Other Local Events

None.

3.2 Server Details

3.2.1 Abstract Data Model

This section describes a conceptual model of possible data organization that an implementation maintains to participate in this protocol. The described organization is provided to facilitate the explanation of how the protocol behaves. This document does not mandate that implementations adhere to this model as long as their external behavior is consistent with that described in this document.

3.2.2 Timers

None.

3.2.3 Initialization

None.

3.2.4 Higher-Layer Triggered Events

None.

3.2.5 Message Processing Events and Sequencing Rules

3.2.5.1 Provision Command

The **Provision** command enables servers to obtain device information from client devices, to send security policy settings set by the server administrator and set a shared policy key, and to send a remote wipe directive.

The Provision command has two phases: an initial phase consisting of a client request followed by an initial server response, then an acknowledgment phase consisting of a client request with an acknowledgment of the initial server response, followed by another server response.

The server SHOULD require that the client device has requested and acknowledged the security policy settings before the client is allowed to synchronize with the server, unless a security policy is set on the server to allow it. The server relies on the client to apply the security policy settings on the client device.

The current security policy settings on the client are represented by a policy key, which SHOULD be received from the client in the X-MS-PolicyKey field of the HTTP header of all protocol command

requests except for the initial **Provision** command, the **Ping** command ([MS-ASCMD] section 2.2.1.11), and the **HTTP OPTIONS** command ([MS-ASHTTP] section 2.2.3). The server generates, stores, and sends the policy key when it responds to a **Provision** command request for policy settings. If the policy key sent by the client does not match the stored policy key, or if the server determines that policy settings must be updated on the client, the server SHOULD<7> return a status code in the next command response indicating that the client needs to send another **Provision** command to request the security policy settings and obtain a new policy key.

The server SHOULD store the device information sent by the client device in a <settings:DeviceInformation> element (specified in [MS-ASCMD] section 2.2.1.16.1) with a **Provision** command request and respond with a **Provision** command response containing a <Status> element (section 2.2.3.2) with the server status value.

The server SHOULD respond to a security policy settings request in an initial **Provision** command request with a <PolicyType> element (section 2.2.3.3) specifying the format of the settings, a <Status> element (section 2.2.3.4) with the server status value, a temporary policy key within a <PolicyKey> element (section 2.2.3.5), and a <Data> type (section 2.2.2.3) containing the current security policy settings. The server responds to the client's acknowledgment **Provision** command request with a <PolicyType> element specifying the format of the settings, a <Status> element with the server status value, and a policy key within a <PolicyKey> element that can be used for subsequent commands.

The server SHOULD respond to an empty initial **Provision** command request with a <Status> element containing the server status value and, if the server has determined that a remote wipe operation should be performed on the client, a remote wipe directive consisting of an empty <RemoteWipe> element (section 2.2.3.48). The server responds to the client's acknowledgment **Provision** command request with a <Status> element with the server status value.

3.2.5.2 Provision Command Errors

Code	Meaning	Cause	Scope	Resolution
1	Success.	The requested policy data is included in the response.	Policy	Apply the policy.
2	Protocol error.	Syntax error in the **Provision** command request.	Global	Fix bug in client code.
2	Policy not defined.	No policy of the requested type is defined on the server.	Policy	Stop sending policy information. No policy is implemented.
3	The policy type is unknown.	The client sent a policy that the server does not recognize.	Policy	Issue a request by using MS-EAS-Provisioning-WBXML.
3	An error occurred on the server.	Server misconfiguration, temporary system issue, or bad item. This is frequently a transient condition.	Global	Retry.
5	Policy key mismatch.	The client is trying to acknowledge an out-of-date or invalid policy.	Policy	Issue a new **Provision** request to obtain a valid policy key.

3.2.6 Timer Events

None.

3.2.7 Other Local Events

None.

4 Protocol Examples

Please note that the sample request/responses do not show the base64-encoding of the **URI** query parameters and WBXML-encoding of the XML bodies for the sake of clarity.

4.1 Downloading the Current Server Security Policy

This section provides a walkthrough of the messages that are used to download the current server security policy. This section contains the following:

- Phase 1: Enforcement
- Phase 2: Client Downloads **Policy** from Server
- Phase 3: Client Acknowledges Receipt and Application of Policy Settings
- Phase 4: Client Performs **FolderSync** by Using the Final <PolicyKey>

4.1.1 Phase 1: Enforcement

In the following example, the client tries the **FolderSync** command, which is denied by the server<8> because the server has determined that the device does not have the current policy (as denoted by the X-MS-PolicyKey header). The server returns HTTP 200 (ok) with a global status code in the body of the response of 142.

Request

```
POST /Microsoft-Server-
ActiveSync?User=deviceuser&DeviceId=6F24CAD599A5BF1A690246B8C68FAE8D&DeviceType=PocketPC&Cmd=
FolderSync HTTP/1.1
Accept-Language: en-us
MS-ASProtocolVersion: 14.0
Content-Type: application/vnd.ms-sync.wbxml
X-MS-PolicyKey: 0
User-Agent: ASOM
Host: EXCH-B-003
<?xml version="1.0" encoding="utf-8"?>
<FolderSync xmlns="FolderHierarchy:">
  <SyncKey>0</SyncKey>
</FolderSync>
```

Response

```
HTTP/1.1 200 OK
Content-Type: application/vnd.ms-sync.wbxml
Date: Mon, 01 May 2006 20:15:15 GMT
Content-Length: 15

<?xml version="1.0" encoding="utf-8"?>
<FolderSync xmlns:A0="AirSync:"
            xmlns:A1="POOMCONTACTS:"
            xmlns:A2="POOMMAIL:"
            xmlns:A3="AirNotify:"
            xmlns:A4="POOMCAL:"
            xmlns:A5="Move:"
            xmlns:A6="GetItemEstimate:"
```

```
            xmlns:A8="MeetingResponse:"
            xmlns:A9="POOMTASKS:"
            xmlns:A10="ResolveRecipients:"
            xmlns:A11="ValidateCert:"
            xmlns:A12="POOMCONTACTS2:"
            xmlns:A13="Ping:"
            xmlns:A14="Provision:"
            xmlns:A15="Search:"
            xmlns:A16="Gal:"
            xmlns:A17="AirSyncBase:"
            xmlns:A18="Settings:"
            xmlns:A19="DocumentLibrary:"
            xmlns:A20="ItemOperations:"
            xmlns:A21="ComposeMail:"
            xmlns:A22="POOMMAIL2:"
            xmlns:A23="Notes:"
            xmlns="FolderHierarchy:">
  <Status>142</Status>
</FolderSync>
```

4.1.2 Phase 2: Client Downloads Policy from Server

In this phase, the client downloads the policy from the server and receives a temporary <PolicyKey>. The client will later use the <PolicyKey> to acknowledge the policy and in doing so obtain a key that will enable the client to successfully execute protocol commands against the server.

Request

```
POST /Microsoft-Server-
ActiveSync?User=deviceuser&DeviceId=6F24CAD599A5BF1A690246B8C68FAE8D&DeviceType=PocketPC&Cmd=
Provision HTTP/1.1
Accept-Language: en-us
MS-ASProtocolVersion: 14.0
Content-Type: application/vnd.ms-sync.wbxml
X-MS-PolicyKey: 0
User-Agent: ASOM
Host: EXCH-B-003

<?xml version="1.0" encoding="utf-8"?>
<Provision xmlns="Provision:">
     <Policies>
          <Policy>
               <PolicyType> MS-EAS-Provisioning-WBXML</PolicyType>
          </Policy>
     </Policies>
</Provision>
```

Response

```
HTTP/1.1 200 OK
Connection: Keep-Alive
Content-Length: 1069
Date: Mon, 01 May 2006 20:15:15 GMT
Content-Type: application/vnd.ms-sync.wbxml
```

```
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
MS-Server-ActiveSync: 8.0
Cache-Control: private

<?xml version="1.0" encoding="utf-8"?>
<Provision xmlns="Provision:">
     <Status>1</Status>
     <Policies>
          <Policy>
               <PolicyType>MS-EAS-Provisioning-WBXML</PolicyType>
               <Status>1</Status>
               <PolicyKey>1307199584</PolicyKey>
               <Data>
                    <eas-provisioningdoc>
                         <DevicePasswordEnabled>1
                         </DevicePasswordEnabled>
                         <AlphanumericDevicePasswordRequired>1
</AlphanumericDevicePasswordRequired> <PasswordRecoveryEnabled>1
                         </PasswordRecoveryEnabled> <DeviceEncryptionEnabled>1
                         </DeviceEncryptionEnabled> <AttachmentsEnabled>1
                         </AttachmentsEnabled> <MinDevicePasswordLength/>
<MaxInactivityTimeDeviceLock>333 </MaxInactivityTimeDeviceLock>
<MaxDevicePasswordFailedAttempts>8 </MaxDevicePasswordFailedAttempts> <MaxAttachmentSize/>
<AllowSimpleDevicePassword>0
                         </AllowSimpleDevicePassword> <DevicePasswordExpiration/>
<DevicePasswordHistory>0
                         </DevicePasswordHistory>
                    </eas-provisioningdoc>
               </Data>
          </Policy>
     </Policies>
</Provision>
```

4.1.3 Phase 3: Client Acknowledges Receipt and Application of Policy Settings

The client acknowledges the policy download and policy application by using the temporary <PolicyKey> obtained in phase 2. In this case, the client has indicated compliance and provided the correct <PolicyKey>. Therefore, the server responds with the "final" <PolicyKey> which the client then uses in the X-MS-PolicyKey header of successive command requests to satisfy policy enforcement.

Request

```
POST /Microsoft-Server-
ActiveSync?User=deviceuser&DeviceId=6F24CAD599A5BF1A690246B8C68FAE8D&DeviceType=PocketPC&Cmd=
Provision HTTP/1.1
Accept-Language: en-us
MS-ASProtocolVersion: 14.0
Content-Type: application/vnd.ms-sync.wbxml
X-MS-PolicyKey: 1307199584
User-Agent: ASOM
Host: EXCH-B-003

<?xml version="1.0" encoding="utf-8"?>
<Provision xmlns="Provision:">
```

```
     <Policies>
          <Policy>
               <PolicyType>MS-EAS-Provisioning-WBXML</PolicyType>
<PolicyKey>1307199584</PolicyKey>
               <Status>1</Status>
          </Policy>
     </Policies>
</Provision>
```

Response

```
HTTP/1.1 200 OK
Connection: Keep-Alive
Content-Length: 63
Date: Mon, 01 May 2006 20:15:17 GMT
Content-Type: application/vnd.ms-sync.wbxml
Server: Microsoft-IIS/6.0
X-Powered-By: ASP.NET
X-AspNet-Version: 2.0.50727
MS-Server-ActiveSync: 8.0
Cache-Control: private

<?xml version="1.0" encoding="utf-8"?>
<Provision xmlns="Provision:">
     <Status>1</Status>
          <Policies>
               <Policy>
                    <PolicyType> MS-EAS-Provisioning-WBXML </PolicyType>
               <Status>1</Status>
               <PolicyKey>3942919513</PolicyKey>
          </Policy>
     </Policies>
</Provision>
```

4.1.4 Phase 4: Client Performs FolderSync by Using the Final PolicyKey

The client uses the "final" policy key obtained in phase 3 in the header of the **FolderSync** command request.

Request

```
POST /Microsoft-Server-
ActiveSync?User=deviceuser&DeviceId=6F24CAD599A5BF1A690246B8C68FAE8D&DeviceType=PocketPC&Cmd=
FolderSync HTTP/1.1
Accept-Language: en-us
MS-ASProtocolVersion: 14.0
Content-Type: application/vnd.ms-sync.wbxml
X-MS-PolicyKey: 3942919513
User-Agent: ASOM
Host: EXCH-B-003

<?xml version="1.0" encoding="utf-8"?>
<FolderSync xmlns="FolderHierarchy:">
     <SyncKey>0</SyncKey>
```

```
</FolderSync>
```

4.2 Directing a Client to Execute a Remote Wipe

The following example shows a set of remote wipe **Requests** and their corresponding **Responses** between a server and a previously provisioned client.

4.2.1 Step 1 Request

```
POST /Microsoft-Server-
ActiveSync?Cmd=FolderSync&User=T0SyncUser1v14.0&DeviceId=Device1&DeviceType=PocketPC HTTP/1.1
Content-Type: application/vnd.ms-sync.wbxml
MS-ASProtocolVersion: 14.0
X-MS-PolicyKey: 0
User-Agent: ASOM
Host: EXCH-B-003

<?xml version="1.0" encoding="utf-8"?>
<FolderSync xmlns="FolderHierarchy:">
     <SyncKey>0</SyncKey>
</FolderSync>
```

4.2.2 Step 1 Response

```
HTTP/1.1 200 OK
Content-Type: application/vnd.ms-sync.wbxml
Date: Wed, 25 Mar 2009 01:23:58 GMT
Content-Length: 15

<?xml version="1.0" encoding="utf-8"?>
<FolderSync >
     <Status>140</Status>
</FolderSync>
```

4.2.3 Step 2 Request

```
POST /Microsoft-Server-
ActiveSync?Cmd=Provision&User=T0SyncUser1v14.0&DeviceId=Device1&DeviceType=PocketPC HTTP/1.1
Content-Type: application/vnd.ms-sync.wbxml
MS-ASProtocolVersion: 14.0
X-MS-PolicyKey: 0
User-Agent: ASOM
Host: EXCH-B-003

<?xml version="1.0" encoding="utf-8"?>
<Provision xmlns="Provision:"></Provision>
```

4.2.4 Step 2 Response

```
HTTP/1.1 200 OK
Content-Type: application/vnd.ms-sync.wbxml
Date: Wed, 25 Mar 2009 01:23:58 GMT
Content-Length: 14
```

```
<?xml version="1.0" encoding="utf-8"?>
<Provision>
<Status>1</Status>
<RemoteWipe />
</Provision>
```

4.2.5 Step 3 Request

```
POST /Microsoft-Server-
ActiveSync?Cmd=Provision&User=T0SyncUser1v14.0&DeviceId=Device1&DeviceType=PocketPC HTTP/1.1
Content-Type: application/vnd.ms-sync.wbxml
MS-ASProtocolVersion: 14.0
X-MS-PolicyKey: 0
User-Agent: ASOM
Host: EXCH-B-003

<?xml version="1.0" encoding="utf-8"?>
<Provision xmlns="Provision:">
    <RemoteWipe>
        <Status>1</Status>
    </RemoteWipe>
</Provision>
```

4.2.6 Step 3 Response

```
HTTP/1.1 200 OK
Content-Type: application/vnd.ms-sync.wbxml
Date: Wed, 25 Mar 2009 01:24:01 GMT
Content-Length: 14

<?xml version="1.0" encoding="utf-8"?>
<Provision>
<Status>1</Status>
</Provision>
```

5 Security

5.1 Security Considerations for Implementers

None.

5.2 Index of Security Parameters

None.

6 Appendix A: Product Behavior

The information in this specification is applicable to the following product versions. References to product versions include released service packs.

- Microsoft® Exchange Server 2007
- Microsoft® Exchange Server 2010
- Microsoft® Exchange Server 2010 SP1 Beta

Exceptions, if any, are noted below. If a service pack number appears with the product version, behavior changed in that service pack. The new behavior also applies to subsequent service packs of the product unless otherwise specified.

Unless otherwise specified, any statement of optional behavior in this specification prescribed using the terms SHOULD or SHOULD NOT implies product behavior in accordance with the SHOULD or SHOULD NOT prescription. Unless otherwise specified, the term MAY implies that product does not follow the prescription.

<1> Section 2.2.3.1: When the MS-ASProtocolVersion header value is 14.0, clients send <settings:DeviceInformation> parameters using the **Settings** command to the server as soon as possible after the client has been provisioned and before the **FolderSync** command so that the server can use this information to determine what the device has access to.

<2> Section 3.1.5.1: Exchange 2007 sends an HTTP 449 response to indicate the client needs to request the security policy settings and obtain a new policy key.

<3> Section 3.1.5.1: Exchange 2007 sends an HTTP 449 response to request a Provision command from the client.

<4> Section 3.1.5.1: Exchange 2007 sends an HTTP 449 response to request a Provision command from the client.

<5> Section 3.1.5.1: Exchange 2007 does not support the <settings:DeviceInformation> element in the **Provision** command from the client and uses the **Settings** command to receive this information.

<6> Section 3.1.5.1: Exchange 2007 sends an HTTP 449 response to initiate a remote wipe on the client.

<7> Section 3.2.5.1: Exchange 2007 sends an HTTP 449 response to indicate the client needs to request the security policy settings and obtain a new policy key.

<8> Section 4.1.1: Exchange 2007 returns status code HTTP 449.

7 Change Tracking

This section identifies changes made to [MS-ASPROV] protocol documentation between February 2010 and May 2010 releases. Changes are classed as major, minor, or editorial.

Major changes affect protocol interoperability or implementation. Examples of major changes are:

- A document revision that incorporates changes to interoperability requirements or functionality.
- An extensive rewrite, addition, or deletion of major portions of content.
- A protocol is deprecated.
- The removal of a document from the documentation set.
- Changes made for template compliance.

Minor changes do not affect protocol interoperability or implementation. Examples are updates to fix technical accuracy or ambiguity at the sentence, paragraph, or table level.

Editorial changes apply to grammatical, formatting, and style issues.

No changes means that the document is identical to its last release.

Major and minor changes can be described further using the following revision types:

- New content added.
- Content update.
- Content removed.
- New product behavior note added.
- Product behavior note updated.
- Product behavior note removed.
- New protocol syntax added.
- Protocol syntax updated.
- Protocol syntax removed.
- New content added due to protocol revision.
- Content updated due to protocol revision.
- Content removed due to protocol revision.
- New protocol syntax added due to protocol revision.
- Protocol syntax updated due to protocol revision.
- Protocol syntax removed due to protocol revision.
- New content added for template compliance.
- Content updated for template compliance.

- Content removed for template compliance.
- Obsolete document removed.

Editorial changes always have the revision type "Editorially updated."

Some important terms used in revision type descriptions are defined as follows:

Protocol syntax refers to data elements (such as packets, structures, enumerations, and methods) as well as interfaces.

Protocol revision refers to changes made to a protocol that affect the bits that are sent over the wire.

Changes are listed in the following table. If you need further information, please contact protocol@microsoft.com.

Section	Tracking number (if applicable) and description	Major change (Y or N)	Revision Type
1.1 Glossary	55129 Added "XML namespace" to the list of terms that are defined in [MS-OXGLOS].	N	Content updated for template compliance.
1.1 Glossary	51246 Added "cabinet file" to the list of terms that are defined in [MS-OXGLOS].	N	Content update.
1.2.1 Normative References	55129 Added reference to [XMLNS].	Y	Content updated for template compliance.
1.3 Overview	Updated the section title.	N	Content updated for template compliance.
1.4 Relationship to Other Protocols	Spelled out protocol name on first use.	N	Content update.
2.2 Message Syntax	54039 Updated XSD for ApplicationName element as optional.	N	Protocol syntax updated.
2.2	54040	N	Protocol

Section	Tracking number (if applicable) and description	Major change (Y or N)	Revision Type
Message Syntax	Updated to specify that Hash child element is optional.		syntax updated.
2.2 Message Syntax	54826 Added DeviceInformation to Provision element.	Y	Content updated due to protocol revision.
2.2 Message Syntax	51247 Updated schema to show request and response separately.	Y	Protocol syntax updated due to protocol revision.
2.2 Message Syntax	55129 Moved XML namespaces table to new Namespaces section.	Y	Content updated for template compliance.
2.2 Message Syntax	54163 Added RemoteWipe element to Provision.	Y	Protocol syntax updated due to protocol revision.
2.2 Message Syntax	47964 Removed unused RequireStorageCardEncryption element.	N	Protocol syntax removed.
2.2 Message Syntax	55308 Clarified optional elements and types in XSD for eas-provisioningdoc child elements.	N	Protocol syntax updated.
2.2.1 Namespaces	55129 Added new section.	Y	Content updated for template compliance.
2.2.2 Complex Types	54163 Added RemoteWipe element to Complex Types.	Y	Content updated due to protocol revision.

Section	Tracking number (if applicable) and description	Major change (Y or N)	Revision Type
2.2.2.2 Policies.Policy	54025 Removed response restriction on Policy.	N	Protocol syntax updated.
2.2.2.4 Policies.Policy.Data.eas-provisioningdoc	54035 Added UnapprovedInROMApplicationList and ApprovedApplicationList child elements to eas-provisioningdoc container element.	Y	Protocol syntax updated.
2.2.2.4 Policies.Policy.Data.eas-provisioningdoc	47964 Removed unused RequireStorageCardEncryption element.	N	Protocol syntax removed.
2.2.2.5 Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList	54913 Added information regarding the scope of "UnapprovedInROMApplicationList".	N	Content update.
2.2.2.5 Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList	54039 Updated to specify that ApplicationName element is optional.	N	Protocol syntax updated.
2.2.2.6 Policies.Policy.Data.eas-provisioningdoc.ApprovedApplicationList	54913 Added information clarifying the scope of the "ApprovedApplicationList" element.	N	Content update.
2.2.2.6 Policies.Policy.Data.eas-provisioningdoc.ApprovedApplicationList	54040 Updated to specify that the Hash child element is optional.	N	Protocol syntax updated.
2.2.2.7 RemoteWipe	54163 Added new section.	Y	New content added due to protocol revision.
2.2.3 Elements	54826 Updated Provision element with new DeviceInformation child element.	Y	New content added due to protocol revision.
2.2.3	54164	Y	New content

Section	Tracking number (if applicable) and description	Major change (Y or N)	Revision Type
Elements	Added RemoteWipe element.		added due to protocol revision.
2.2.3 Elements	47964 Removed unused RequireStorageCardEncryption element.	N	Protocol syntax removed.
2.2.3 Elements	54098 Clarified description of DevicePasswordHistory element.	N	Content update.
2.2.3 Elements	51246 Changed "CAB file" to "cabinet file" to match term in glossary.	N	Editorially updated.
2.2.3.1 DeviceInformation	54826 Added section for new DeviceInformation child element to Provision command.	Y	New content added due to protocol revision.
2.2.3.2 Status	51234 Updated description of Status element contents to include failures.	N	Protocol syntax updated.
2.2.3.4 Policies.Policy.Status	51234 Updated description of Status element contents to include failures.	N	Content update.
2.2.3.4 Policies.Policy.Status	54060 Changed parent of Status element from "Status" to "Policies.Policy".	N	Content update.
2.2.3.6 Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled	51250 Clarified number of DevicePasswordEnabled elements allowed.	N	Protocol syntax updated.
2.2.3.6 Policies.Policy.Data.eas-provisioningdoc.DevicePasswordEnabled	55307 Clarified meaning of DevicePasswordEnabled values.	N	Protocol syntax updated.
2.2.3.7 Policies.Policy.Data.eas-provisioningdoc.AlphaNumericDevicePasswordRequired	55307 Clarified meaning of AlphaNumericDevicePasswordRequired values.	N	Content update.

Section	Tracking number (if applicable) and description	Major change (Y or N)	Revision Type
2.2.3.7 Policies.Policy.Data.eas-provisioningdoc.AlphaNumericDevicePasswordRequired	55308 Clarified description of optional element quantities.	N	Protocol syntax updated.
2.2.3.8 Policies.Policy.Data.eas-provisioningdoc.PasswordRecoveryEnabled	54757 Updated specification of server behavior.	N	Content update.
2.2.3.8 Policies.Policy.Data.eas-provisioningdoc.PasswordRecoveryEnabled	55308 Clarified description of optional element quantities.	N	Content update.
2.2.3.8 Policies.Policy.Data.eas-provisioningdoc.PasswordRecoveryEnabled	55307 Clarified description of PasswordRecoveryEnabled element values.	N	Content update.
2.2.3.9 Policies.Policy.Data.eas-provisioningdoc.DeviceEncryptionEnabled	55308 Clarified description of optional element quantities.	N	Protocol syntax updated.
2.2.3.9 Policies.Policy.Data.eas-provisioningdoc.DeviceEncryptionEnabled	55307 Clarified meaning of DeviceEncryptionEnabled values.	N	Content update.
2.2.3.10 Policies.Policy.Data.eas-provisioningdoc.AttachmentsEnabled	55307 Clarified description of AttachmentsEnabled values.	N	Content update.
2.2.3.10 Policies.Policy.Data.eas-provisioningdoc.AttachmentsEnabled	55308 Clrified description of optional element quantities.	N	Content update.
2.2.3.11 Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordLength	55308 Clarified description of optional element quantities.	N	Content update.
2.2.3.12 Policies.Policy.Data.eas-provisioningdoc.MaxInactivityTimeDeviceLock	55308 Clarified description of optional element quantities.	N	Content update.
2.2.3.12 Policies.Policy.Data.eas-provisioningdoc.MaxInactivityTimeDeviceLock	55307 Clarified meaning of MaxInactivityTimeDeviceLock values.	N	Content update.
2.2.3.13 Policies.Policy.Data.eas-provisioningdoc.MaxDevicePasswordFailedAttempts	54093 Updated range of MaxDevicePasswordFailedAttempts element contents.	N	Protocol syntax updated.
2.2.3.13	47983	N	Content

Section	Tracking number (if applicable) and description	Major change (Y or N)	Revision Type
Policies.Policy.Data.eas-provisioningdoc.MaxDevicePasswordFailedAttempts	Updated description of client behavior for MaxDevicePasswordFailedAttempts element.		update.
2.2.3.13 Policies.Policy.Data.eas-provisioningdoc.MaxDevicePasswordFailedAttempts	55308 Clarified description of optional element quantities.	N	Content update.
2.2.3.14 Policies.Policy.Data.eas-provisioningdoc.MaxAttachmentSize	55308 Specified that MaxAttachmentSize child element is optional.	N	Protocol syntax updated.
2.2.3.15 Policies.Policy.Data.eas-provisioningdoc.AllowSimpleDevicePassword	Clarified meaning of simple password.	N	Content update.
2.2.3.15 Policies.Policy.Data.eas-provisioningdoc.AllowSimpleDevicePassword	55308 Clarified description of optional element quantities.	N	Content update.
2.2.3.16 Policies.Policy.Data.eas-provisioningdoc.DevicePasswordExpiration	49004 Updated DevicePasswordExpiration element description as number of days before a password expires.	N	Protocol syntax updated.
2.2.3.16 Policies.Policy.Data.eas-provisioningdoc.DevicePasswordExpiration	55308 Clarified description of optional element quantities.	N	Content update.
2.2.3.17 Policies.Policy.Data.eas-provisioningdoc.DevicePasswordHistory	54098 Clarified description of content of DevicePasswordHistory element.	N	Content update.
2.2.3.17 Policies.Policy.Data.eas-provisioningdoc.DevicePasswordHistory	55308 Clarified description of optional element quantities.	N	Content update.
2.2.3.18 Policies.Policy.Data.eas-provisioningdoc.AllowStorageCard	54068 Updated to specify AllowStorageCard child element is optional.	N	Protocol syntax updated.
2.2.3.18 Policies.Policy.Data.eas-provisioningdoc.AllowStorageCard	55308 Clarified description of optional element quantities.	N	Content update.
2.2.3.19 Policies.Policy.Data.eas-provisioningdoc.AllowCamera	54069 Deleted statement that the parent could have 0 or 1 instances of this element.	N	Content update.

Section	Tracking number (if applicable) and description	Major change (Y or N)	Revision Type
2.2.3.19 Policies.Policy.Data.eas-provisioningdoc.AllowCamera	55308 Clarified description of optional element quantities.	N	Content update.
2.2.3.20 Policies.Policy.Data.eas-provisioningdoc.RequireDeviceEncryption	54070 Deleted statement saying that the parent could have 0 or 1 instance of this element.	N	Editorially updated.
2.2.3.20 Policies.Policy.Data.eas-provisioningdoc.RequireDeviceEncryption	55308 Clarified description of optional element quantities.	N	Content update.
2.2.3.21 Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedApplications	54072 Deleted statement that the parent element could have 0 or 1 instance of this element.	N	Editorially updated.
2.2.3.21 Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedApplications	55308 Clarified description of optional element quantities.	N	Content update.
2.2.3.22 Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedInstallationPackages	54073 Deleted statement that parent element could have 0 or 1 instance of this element.	N	Editorially updated.
2.2.3.22 Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedInstallationPackages	51246 Changed "CAB file" to "cabinet file" to match term in glossary.	N	Content update.
2.2.3.22 Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedInstallationPackages	55308 Clarified description of optional element quantities.	N	Content update.
2.2.3.22 Policies.Policy.Data.eas-provisioningdoc.AllowUnsignedInstallationPackages	55307 Clarified meaning of AllowUnsignedInstallationPackages values.	N	Content update.
2.2.3.23 Policies.Policy.Data.eas-provisioningdoc.MinDevicePasswordComplexCharacters	55308 Changed description of the MinDevicePasswordComplexCharacters element from required to optional.	N	Content update.
2.2.3.24 Policies.Policy.Data.eas-provisioningdoc.AllowWifi	55308 Changed description of the AllowWifi element from required to opitional.	N	Content update.
2.2.3.25 Policies.Policy.Data.eas-	55308 Clarified description of optional	N	Content

Section	Tracking number (if applicable) and description	Major change (Y or N)	Revision Type
provisioningdoc.AllowTextMessaging	element quantities.		update.
2.2.3.26 Policies.Policy.Data.eas-provisioningdoc.AllowPOPIMAPEmail	55308 Changed description of element from required to optional.	N	Content update.
2.2.3.27 Policies.Policy.Data.eas-provisioningdoc.AllowBluetooth	55308 Changed description of AllowBluetooth element from required to optional.	N	Content update.
2.2.3.28 Policies.Policy.Data.eas-provisioningdoc.AllowIrDA	55308 Changed description of AllowIrDA element from required to optional.	N	Content update.
2.2.3.29 Policies.Policy.Data.eas-provisioningdoc.RequireManualSyncWhenRoaming	54104 Clarified description of RequireManualSyncWhenRoaming values.	N	Content update.
2.2.3.29 Policies.Policy.Data.eas-provisioningdoc.RequireManualSyncWhenRoaming	55308 Changed description of RequireManualSyncWhenRoaming element from required to optional.	N	Content update.
2.2.3.30 Policies.Policy.Data.eas-provisioningdoc.AllowDesktopSync	55308 Changed description of the AllowDesktopSync element from required to optional.	N	Content update.
2.2.3.31 Policies.Policy.Data.eas-provisioningdoc.MaxCalendarAgeFilter	55308 Changed description of the MaxCalendarAgeFilter element from required to optional.	N	Content update.
2.2.3.32 Policies.Policy.Data.eas-provisioningdoc.AllowHTMLEmail	55308 Changed description of the AllowHTMLEmail element from required to optional.	N	Content update.
2.2.3.32 Policies.Policy.Data.eas-provisioningdoc.AllowHTMLEmail	55307 Clarified meaning of AllowHTMLEmail values.	N	Content update.
2.2.3.33 Policies.Policy.Data.eas-provisioningdoc.MaxEmailAgeFilter	55308 Changed description of the MaxEmailAgeFilter element from required to optional.	N	Content update.
2.2.3.34 Policies.Policy.Data.eas-	55308 Changed description of the	N	Content update.

Section	Tracking number (if applicable) and description	Major change (Y or N)	Revision Type
provisioningdoc.MaxEmailBodyTruncationSize	MacEmailBodyTruncationSize element from required to optional.		
2.2.3.35 Policies.Policy.Data.eas-provisioningdoc.MaxEmailHTMLBodyTruncationSize	55308 Changed description of the MaxEmailHTMLBodyTruncationSize element from required to optional.	N	Content update.
2.2.3.36 Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEMessages	55308 Changed description of the RequireSignedSMIMEMessages element from required to optional.	N	Content update.
2.2.3.36 Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEMessages	55307 Clarified meaning of RequireSignedSMIMEMessages values.	N	Content update.
2.2.3.37 Policies.Policy.Data.eas-provisioningdoc.RequireEncryptedSMIMEMessages	55307 Clarified meaning of RequireEncryptedSMIMEMessages values.	N	Content update.
2.2.3.37 Policies.Policy.Data.eas-provisioningdoc.RequireEncryptedSMIMEMessages	55308 Changed description of the RequireEncryptedSMIMEMessages element from required to optional.	N	Content update.
2.2.3.38 Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEAlgorithm	54112 Changed name of encryption algorithm from "SHA" to "SHA1".	N	Content update.
2.2.3.38 Policies.Policy.Data.eas-provisioningdoc.RequireSignedSMIMEAlgorithm	55308 Changed description of the RequireSignedSMIMEAlgorithm element from required to optional.	N	Content update.
2.2.3.39 Policies.Policy.Data.eas-provisioningdoc.RequireEncryptionSMIMEAlgorithm	54113 Changed name of algorithm from "3DES" to "TripleDES".	N	Content update.
2.2.3.39 Policies.Policy.Data.eas-provisioningdoc.RequireEncryptionSMIMEAlgorithm	55308 Changed description of the RequireEncryptionSMIMEAlgorithm element from required to optional.	N	Content update.
2.2.3.40	55308	N	Content

Section	Tracking number (if applicable) and description	Major change (Y or N)	Revision Type
Policies.Policy.Data.eas-provisioningdoc.AllowSMIMEEncryptionAlgorithmNegotiation	Changed description of the AllowSMIMEEncryptionAlgorithmNegotiation element from required to optional.		update.
2.2.3.41 Policies.Policy.Data.eas-provisioningdoc.AllowSMIMESoftCerts	55308 Changed description of the AllowSMIMESoftCerts element from required to optional.	N	Content update.
2.2.3.41 Policies.Policy.Data.eas-provisioningdoc.AllowSMIMESoftCerts	55307 Clarified meaning of AllowSMIMESoftCerts values.	N	Content update.
2.2.3.42 Policies.Policy.Data.eas-provisioningdoc.AllowBrowser	55308 Changed description of the AllowBrowser element from required to optional.	N	Content update.
2.2.3.43 Policies.Policy.Data.eas-provisioningdoc.AllowConsumerEmail	51251 Updated description of policy values.	N	Content update.
2.2.3.43 Policies.Policy.Data.eas-provisioningdoc.AllowConsumerEmail	55308 Changed description of the AllowConsumerEmail element from required to optional.	N	Content update.
2.2.3.44 Policies.Policy.Data.eas-provisioningdoc.AllowRemoteDesktop	55308 Changed description of the AllowRemoteDesktop element from required to optional.	N	Content update.
2.2.3.45 Policies.Policy.Data.eas-provisioningdoc.AllowInternetSharing	55308 Changed description of the AllowInternetSharing element from required to optional.	N	Content update.
2.2.3.46 Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList.ApplicationName	54913 Added information clarifying the scope of "ApplicationName" element.	N	Content update.
2.2.3.46 Policies.Policy.Data.eas-provisioningdoc.UnapprovedInROMApplicationList.ApplicationName	54039 Clarified description of ApplicationName element as optional.	N	Content update.
2.2.3.47 Policies.Policy.Data.eas-provisioningdoc.ApprovedApplicationList.Hash	54913 Added information to clarify the scope of the "Hash" element.	N	Content update.
2.2.3.47	54040	N	Content

Section	Tracking number (if applicable) and description	Major change (Y or N)	Revision Type
Policies.Policy.Data.eas-provisioningdoc.ApprovedApplicationList.Hash	Clarified description of Hash element as optional.		update.
2.2.3.48 RemoteWipe	54163 Added new section for RemoteWipe element.	Y	New content added due to protocol revision.
2.2.3.49 RemoteWipe.Status	54163 Added new section for Status child element of RemoteWipe complex type.	Y	New content added due to protocol revision.
3.1.1 Abstract Data Model	51345 Moved protocol details to Message Processing Events and Sequencing Rules section.	Y	Content update.
3.1.5.1 Provision Command	51345 Updated content moved from Abstract Data Model section for protocol revision.	Y	Content updated due to protocol revision.
3.1.5.2 Provision Command Errors	54063 Removed unused status code 4.	N	Content update.
3.2.1 Abstract Data Model	51345 Moved protocol details to Message Processing Events and Sequencing Rules.	Y	Content updated due to protocol revision.
3.2.5.1 Provision Command	51345 Updated content moved from Abstract Data Model section for protocol revision.	Y	Content updated due to protocol revision.
3.2.5.2 Provision Command Errors	54063 Removed unused status code 4.	N	Content update.
4.1.1 Phase 1: Enforcement	54155 Added missing items from sample request header.	N	Content update.
4.1.1 Phase 1: Enforcement	51241 Added sample response.	N	Content update.

Section	Tracking number (if applicable) and description	Major change (Y or N)	Revision Type
4.1.2 Phase 2: Client Downloads Policy from Server	54156 Corrected sample request.	N	Content update.
4.1.3 Phase 3: Client Acknowledges Receipt and Application of Policy Settings	54157 Corrected sample request.	N	Content update.
4.1.4 Phase 4: Client Performs FolderSync by Using the Final PolicyKey	54158 Corrected sample request.	N	Content update.
4.2 Directing a Client to Execute a Remote Wipe	54159 Clarified description of example.	Y	Editorially updated.
4.2.2 Step 1 Response	53445 Removed header "X-MS-MV: 14.0.511" from protocol example.	N	Content update.
4.2.3 Step 2 Request	54160 Added xmlns namespace attribute to Provision command element.	N	Content update.
4.2.4 Step 2 Response	53445 Removed header "X-MS-MV: 14.0.511" from protocol example.	N	Content update.
4.2.5 Step 3 Request	54161 Added Provision namespace.	N	Content update.
4.2.6 Step 3 Response	53445 Removed header "X-MS-MV: 14.0.511" from protocol example.	N	Content update.
4.2.6 Step 3 Response	54162 Removed <RemoteWipe /> from response.	N	Content update.
2.2.3.21 Policies.Policy.Data.eas-provisioningdoc.RequireStorageCardEncryption	47964 Removed section for unused RequireStorageCardEncryption element.	Y	Content removed.

8 Index